# Detailed Analysis of Current Trust Agreements

## September 29, 2017

AUDACIOUS INQUIRY | BOLD SOLUTIONS FOR CONNECTED HEALTHCARE

# Background

- The finding of the analysis are based on review of the included organization's:
  - Legal agreements;
  - Bylaws;
  - Policies and procedures;
  - Accreditation programs;
  - Technical testing programs; and
  - Use cases.
- The included organizations were given an opportunity to review and provide input on the findings.
- This analysis was created by Audacious Inquiry, LLC under a contract with the Office of the National Coordinator for Health Information Technology (ONC). The content, views, and opinions do not necessarily reflect those of the Department of Health and Human Services or ONC.

# TRUST CATEGORY: Purpose & Scope of Arrangements

## SUB-CATEGORY: Goal

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Develop a comprehensive policy and operational framework, with a common legal agreement, to enable seamless exchange across different health data sharing networks, programs, and services. | Health data should be available to individuals and providers regardless of where care occurs, and access to that data must be built into health IT tools at a reasonable cost to enable use by a broad range of health care providers and the people they serve. | To support health information exchange that is secure, interoperable, affordable, and widely available, in the interest of the public good, and to do so as a non-profit, competitively neutral, membership 'learning organization' for voluntary self-governance of health information exchange. | Create a trusted exchange framework, using a common legal agreement (the DURSA), to support the secure exchange of health information in a technology agnostic manner, over the Internet, using a standardized approach that works across diverse geographies, architectures, and technology platforms. | Address the legal, policy, and technical barriers that inhibit health information exchange between data holders and healthcare consumers. | Ensure that all patients have their complete, longitudinal health records available wherever and whenever it is needed for decisions about their care through a network of nationwide patient-centered, location-independent, and proactive interoperability. PCDH connects participating HIEs to enable the secure sharing of patient health information across state lines and across health systems, improving the patient experience by making their health information available to authorized providers for care and "centered" around the patient. | A national digital healthcare infrastructure and network for the exchange of health information, including prescription and medication information, Direct messages, and medical records through a national record locator service. A secure and neutral network in which all stakeholders meeting specified certification and implementation requirements could participate with the assurance that their information will be transmitted accurately, timely, and securely. |

# TRUST CATEGORY: Purpose & Scope of Arrangements

## SUB-CATEGORY: Scope of Exchange

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Currently live with an initial use case of Query-Based Document Exchange, to enable network-to-network directed queries/responses among participants. | Vendor-neutral platform that facilitates data exchange among participating implementers. | Push exchange across participating Health Information Service Providers (HISPs). | Directed data query/response among participants. | Consumer mediated exchange via the Direct Protocols. NATE seeks to implement solutions to facilitate the ability of consumers to receive their information from HIPAA covered entities via Direct to a consumer facing applications of the consumer's choice. | Pushed alerts based on care events occurring in a remote HIO pushed to the patient's home HIO to establish identity resolution, acknowledgement of matched identities and subsequent query/response among participating HIOs. | Query/response and push. |

# TRUST CATEGORY: Purpose & Scope of Arrangements

## SUB-CATEGORY: Approach to Establishing Trust

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Legal agreements, participant data exchange testing. | Legal agreements, certification and onboarding process, network monitoring and reporting. | Legal agreements, accreditation and audit of service providers, participant data exchange testing, and Public Key Infrastructure. | Legal agreements, certification program. | Legal agreements, self-attestation. | Legal agreements. | Legal agreements, certification program, compliance and enforcement program. |

# TRUST CATEGORY: Purpose & Scope of Arrangements

## SUB-CATEGORY: Governance Structure

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Carequality is governed by a Steering Committee, which has responsibility for the overall governance and strategic direction. Applications are solicited annually for members of the Steering Committee. The Steering Committee consults an Advisory Council, to allow for broader stakeholder input, on issues relating to the Carequality Framework. At any given time, there typically are lower-level working groups actively engaged in the details of developing and maintaining components of the Carequality framework. These groups provide draft work products to the Advisory Council, which after further discussion and refinement will pass the work to the Steering Committee with a recommendation to adopt it. | CommonWell is governed by a Board of Directors, which has responsibility for overall governance and strategic direction. There is also the CommonWell Advisory Board, of provider representatives, that articulates end-user feedback. CommonWell operates through eight committees that advise the Board of Directors including:<br>• Operating<br>• Marketing<br>• Membership<br>• Government Affairs<br>• Privacy & Security<br>• Use Case<br>• Standards, Technology & Implementation<br>• Deployment & Utilization | DirectTrust is governed by a Board of Directors that has responsibility for overall governance and strategic direction. DirectTrust has six active workgroups that advise the Board of Directors:<br>• Certificate Policy and Practices Workgroup<br>• Direct Directory Policy Workgroup<br>• DirectTexting Workgroup<br>• FHIR Security and Trust Workgroup<br>• Patient and Consumer Participation in Direct Workgroup<br>• Security and Trust Compliance Workgroup | eHealth Exchange is governed by the Coordinating Committee which has responsibility for overall oversight and management of eHealth Exchange and for supporting participants. Membership on the committee is representative of the participants. The Coordinating Committee has three advisory bodies and may convene others as needed:<br>• Specifications Work Group<br>• Policy and Technical Task Group<br>• Testing Work Group | NATE is governed by a Board of Directors, which has responsibility for overall governance and strategic direction. Committees of the Board include:<br>• Membership Committee | The SHIEC PCDH is governed by the PCDH Governance Council which approves policies and procedures related to among other things:<br>i. the governance of the PCDH<br>ii. technical, data format and content specifications;<br>iii. the conduct of PCDH activities;<br>iv. access to Data; and<br>v. the protection of PHI and Confidential Information.<br>HIOs must participate with a 'Region' of their peers to participate in nationwide PCDH. Each participating Region appoints two members to the Council. | Surescripts is governed by a Board of Directors. |

# TRUST CATEGORY: Purpose & Scope of Arrangements

## SUB-CATEGORY: Operational Policies/Procedures

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Operational policies and procedures may be defined directly in a use case Implementation Guide, but will typically be defined in separate document. Policy and procedures for technical security and certificate use, for example, are outlined in Carequality's Technical Trust Policy document. http://sequoiaproject.org/carequality/resources/ | CommonWell has a variety of operating policies including: Data Privacy and Security Policy and Statement of Information Handling Practices, Data Retention Policy, Conflicts of Interest Policy, Whistleblower Policy, Use Case Approval Process. http://www.commonwellalliance.org/data-and-security/ | DirectTrust has a variety of operating policies including a HIISP Policy, a Certificate Policy, a Directory Data Sharing Policy, and standard operating procedures for its trust anchor bundles. https://www.directtrust.org/about-policies/ | eHealth Exchange has a variety of operating policies and procedures including DURSA Amendment Process, Review and Disposition of Applications for Participation, Change Process-Operating Policies and Procedures. http://sequoiaproject.org/wp-content/uploads/2017/06/2017-06-15-ehealth-exchange-opps.zip | NATE has a variety of policies and procedures including Membership Eligibility, and Onboarding to a Trust Profile. http://nate-trust.org/work-products/ | The PCDH Governance Council has the authority to develop nationwide operational policies and procedures, and Regions have the authority to develop Region-specific operational policies and procedures. | Surescripts has a Certification Guide, Network Operations Guide and Implementation Guide. |

# TRUST CATEGORY: Permitted Purposes for Data Exchange

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Permitted purposes are established in each Implementation Guide (i.e. use case) and can vary across Implementation Guides. Differing policies can also be associated with individual permitted purposes in an Implementation Guide (i.e. treatment). In the initial Query-Based Document Exchange Implementation Guide the following permitted purposes are allowed:<br>• Treatment<br>• Payment<br>• Health Care Operations<br>• Public Health Activities<br>• Authorization Based Disclosures | Permitted purposes are:<br>• Treatment<br>• Patient access | DirectTrust leverages the HIPAA Privacy Rules permitted disclosures framework which allows a covered entity to exchange data for the following purposes without authorization:<br>• Treatment<br>• Payment<br>• Operations | Permitted purposes are defined at the network level and are:<br>• Treatment<br>• Payment (for a provider)<br>• Operations (limited compared to HIPAA)<br>• Public Health Activities<br>• Any purpose to demonstrate Meaningful Use<br>• Uses and disclosures pursuant to an authorization | Participants shall only transmit data as directed or approved by the consumer. | Permitted purposes are:<br>• Treatment<br>• Care coordination, care or case management, and transition of care planning; and<br>• Such other purposes as may be approved as an amendment by the PCDH Governance Council, so long as such purpose is permitted by Applicable Law. Regions can establish more or less permissive permitted purposes. | Treatment purposes. |

# TRUST CATEGORY: **Permitted Participants**

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Permitted users are identified in each Implementation Guide. In the initial Query-Based Document Exchange Implementation Guide no limitations were placed on permitted users, as long as the user can appropriately claim a permitted purpose for the query. Examples of participants include: government agencies, health IT developers, HIOs, national networks, and their end users. | CommonWell members that are health IT developers can subscribe to CommonWell Services and enable their end users to access services through the developer's product. | Participants typically are health IT developers, HISPs, certificate authorities, registration authorities, government agencies, HIOs, and their end users which include hospitals, medical practices, and other organizations providing care or supporting care processes. Patients may also participate. | Participants must be a valid legal entity, have the ability to govern the use of its network, sign the DURSA, have the ability to enforce the flow-down provisions in the DURSA and pass applicable testing. | Participants are "consumer facing application" which for NATE includes any application that is patient controlled and uses Direct to receive protected health information from external systems. The application may be web-based, mobile or both. It includes what have been traditionally described as PHRs as well as more narrowly focused consumer controlled apps that use the Direct mode of exchange as a secure transport mechanism between the consumer and the sources of PHI about them, including their caregivers, payers and government entities. | Approved SHIEC HIO members and their end users. SHIEC HIO members must be sponsored by a participating Region and receive approval from the PCDH Governance Council to participate. The Governance Council is allowed to make exceptions to the membership rule. | Participants include<br>i. authorized and licensed providers and pharmacy benefit management companies and<br>ii. technology vendors and other aggregators of providers; all of whom have entered into written agreements with Surescripts, either directly or indirectly, in order to access or communicate through the Surescripts network. |

# TRUST CATEGORY: Identity Proofing & Authentication



| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Carequality participants or appropriate designees such as their customers/members, are required to validate the identity of any end users who have access to exchange functionality via Carequality. Participating systems - as distinct from individual end users - are identified at a technical level by an x.509 certificate issued by The Sequoia Project and specific to Carequality. The Sequoia Project's certificate authority meets FBCA requirements, including those related to identity-proofing of the "Subscriber" who is responsible for handling of the x.509 certificate. | • Participants are responsible for user authentication and authorization for access to the services prior to transacting with CommonWell.<br>• Participants are responsible for management of customer organizational registration with CommonWell<br>• Edge systems are responsible for managing the status of user qualifications to both locally authorize and accordingly locally audit, and to report any adverse changes upstream.<br>• CommonWell uses x.509 certificates. Certificate Authority must be certified by WebTrust. | HISPs, Certificate Authorities, and Registration Authorities participating in a trust bundle are legally bound to the terms and requirements of the specific trust bundle, which among other things specify the level of assurance (LOA) of identity proofing and verification required of end users. The minimum LOA tied to a trust bundle is currently NIST LOA 3. For the Governmental Trust Anchor Bundle the minimum LOA is FBCA Medium. As part of accreditation CAs and RAs are audited on their identity proofing of end users. DirectTrust does not specify levels of authentication to end user systems (e.g. EHRs, PHRs) but it has issued recommendations that multi-factor authentication is the preferred approach. DirectTrust uses x.509 digital certificates. | Participants are required to have processes in place to identity proof users and authenticate users. The eHealth Exchange issues digital credentials (x.509 digital certificates) to an authorized representative of the Participant, who is identity-proofed and who accepts responsibility for the secure use and management of the Participant's digital credentials. The certificate authority used for the eHealth Exchange is cross-certified to the federal bridge. | Participants shall conform to industry-accepted security practices and at a minimum maintain necessary safeguards for ensuring the privacy and security of personally identifiable health information. | Participants shall employ a process by which the participant, or its designee, validates sufficient information to uniquely identify each end user seeking to use its system prior to issuing digital credentials. Participants shall employ a process by which the participant, or its designee, uses the digital credentials to verify the identity of each end user prior to enabling them to exchange data. | Generally, technology vendors and health systems are required to conduct, or are required to cause their customers to conduct, identity proofing and authentication sufficient to meet regulatory requirements and industry standards to Surescripts' reasonable satisfaction to confirm that all messages transmitted via the Surescripts network originate from duly authorized providers who are licensed to use the application for the service(s) for which Surescripts has certified the application, and who are registered with the technology vendor in accordance with the terms and conditions of their agreement with Surescripts. |

# TRUST CATEGORY: Technical Approach & Infrastructure

## SUB-CATEGORY: Technical Approach

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC strategichie.com Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Implementation Guides and supporting documentation referenced by the Guides specify the technical approach for a particular use case. While specific approaches may vary by use case, under the current Implementation Guide for Query-Based Document Exchange Carequality has taken a federated approach to the architecture. | CommonWell has a single set of specifications that participants must use to exchange data over the network. CommonWell provides centralized infrastructure to support patient enrollment, record location, patient identification and linking, and data brokering for federated data query and retrieval. CommonWell infrastructure does not include a Clinical Data Repository. | DirectTrust has a single set of specifications that participants must use to exchange data over the network. DirectTrust supports push based exchange of health information via the Direct Protocol and provides enabling support infrastructure. The Direct Protocol includes specifications for: backbone transport and universal addressing; messaging gateway; security and trust; edge protocols; and source and destination clients. | eHealth Exchange has adopted a set of specifications for profiles supported by the network. Participants must use the applicable specifications for the profiles they opt to support. Testing is required for some, but not all profiles. Participants are required to test for compliance with the technical specifications for their selected profiles when testing is required. eHealth Exchange has a federated architecture. | NATE has a single set of specifications that participants must use to exchange data over the network. NATE supports push based exchange of health information via the Direct Protocol and provides enabling support infrastructure. | SHIEC has a set of specifications that participants must use to exchange data over the network. With approval of the PCDH Governing Board additional standards can be added overtime. Regions may have different use cases and take differing technical approaches to enabling exchange among participants of the Region. SHIEC's general interoperability approach is to 1) trigger alerts based on care events occurring in a remote HIO that is pushed to the patient's local or "Home" HIO so that 2) precisely where and when the patient received care, as well as their identity might be accurately resolved and 3) local HIE governance policies are then applied, and if permitted, alerting is delivered to relevant providers, records returned to the remote HIE to support care of the patient and 4) the home HIE can query and receive the final records when the patient is back home. | Surescripts has a Pharmacy Aggregator Master Agreement and a Prescriber Connectivity agreement. Aggregators must engage in contracts, undergo certification and network testing to access the network. |

# TRUST CATEGORY: Technical Approach & Infrastructure

## SUB-CATEGORY: Standards Used

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Standards used vary by use case. Key standards currently in use include: XCPD, XCA, TLS, C-CDA, SAML, and FHIR. | PIX, FHIR, REST, XCA, XUA, SAML, C-CDA, and TLS/SSL | Direct Protocol | Standards used vary by the profile supported by the participant. Key standards adopted include: XCPD, XCA, BPPC, XUA, ATNA, TLS, C-CDA, SAML, FHIR, NCPDP, PMIX, SCRIPT, HL7 v2, and Direct. | Direct Protocol | Key standards used include: HL-7 2.x ADT, HL-7 2.x, CCDA 2.x, DICOM, sFTP, VPN, and Web services. | NCPDP SCRIPT, NCPDP Formulary and Benefit, X12 270/271, and Direct. |

# TRUST CATEGORY: Technical Approach & Infrastructure

## SUB-CATEGORY: Infrastructure

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| The Carequality Directory includes endpoint address information of Carequality participants and identifies which use cases they participate in and the role they play (i.e. query responded and initiator, query responder etc.). For the Query-Based Document Exchange use case, participants have the option to leverage an record locator service (RLS), with the use case providing for the potential of multiple competing RLS offerings. | Centralized infrastructure for consent management/ enrollment, identity management, record location, and brokering for data query and retrieval. | Multiple trust bundles and an optional Direct address directory. | Service registry directory that includes endpoint information of participants and identifies the profiles supported, geographic coverage area and other pertinent information so that participants can find exchange partners. | Trust bundle | Methods vary by Region. Point-to-point connections enable alerting within two of the Regions, and one Region utilizes a central hub to connect its participants. The Regions are connected to one another via a hub or a single regional member acting as a gateway. | Foundation infrastructure including interface specifications, transaction routing infrastructure, participant management services, and error management services. MPI and Provider Directory. |

# TRUST CATEGORY: Cooperation & Non-Discrimination

| carequality | commonwell HEALTH ALLIANCE | DirectTrust |
|---|---|---|
| Carequality has overall provisions that prohibit discrimination against particular participants or groups of participants, with respect to information exchange. Each use case Implementation Guide outlines specific interpretations of the non-discrimination policy relevant to that use case. For the Query-Based Document Exchange Implementation Guide participants are prohibiting from requiring additional fees, terms, or conditions on other participants for queries or responses related to treatment purposes. In addition, Carequality requires participants to treat different participants in a similar manner for the same permitted purpose (e.g. if queries for payment are accepted under particular terms from one payer, they must be accepted from any payer willing to meet similar terms). | Cooperation and non-discrimination requirements are incorporated as required into Use Case Requirements and Specifications; for example, as pre-conditions to the HIPAA treatment use case. Network activity is monitored so that improper behavior can be detected and remediated. | Except for routine maintenance or as necessary to conform to the participant's trust constraints (e.g. if the sender's trust certificate has expired), a participant is prohibited from intentionally preventing or delaying an incoming or outgoing exchange of a conformant Direct message with another participant. Participants also agree to not engage in information blocking as defined in the 21st Century Cures Act and any implementing regulations. |

# TRUST CATEGORY: Cooperation & Non-Discrimination - 2

| eHealth Exchange | NATE | SHIEC | surescripts |
|---|---|---|---|
| Participants who query for treatment purposes have a duty to respond to requests for data for treatment purposes from other participants with either a copy of the requested data or a standardized response that data is not available unless there is cause to believe that a Participant is not complying with eHealth Exchange requirements. Participants have the option to respond to queries for other permitted purposes. | N/A | Members will cooperate with each other in the development, installation, support and operation of interfaces in accordance with the technical, data format and content specifications set forth in the policies and procedures. The interfaces will allow participants to exchange data consistent with permitted purposes. Participants or Regions permitted purposes may differ as a result of differing member participant agreements, applicable law, and business practices. Based on these differences participants may make different determinations of whether and how to exchange data with other participants. Participants are required to make a good faith effort to exchange data for permitted purposes outlined in the agreement. Each member must comply with applicable regulatory requirements.<br><br>It is the intent of the participants that an interface not be used by a participant's end users in a manner that allows the end user to avoid supporting a HIO in the geographic area served by a participant where the end users' medical facilities are located. If any participant believes that an interface is being used in this manner, the impacted participant shall notify the PCDH Governance Council. The appropriate participants and the PCDH Governance Council will work together in good faith to address such concerns. If the appropriate participants and PCDH Governance Council cannot agree on how to address such concerns, the impacted participant may disallow use of the interface by the relevant end user of the other participant. | Participants must comply with the terms and conditions of the applicable agreements and associated artifacts (certification guide, etc.). A participant retains the right to not exchange information with another participant. |

# TRUST CATEGORY: Accountability

## SUB-CATEGORY: Technical Accountability Mechanism

| carequality | commonwell HEALTH ALLIANCE | DirectTrust |
|---|---|---|
| Each use case may specify validation steps to be completed. For the Query-Based Document Exchange use case, participating network and service operators (as opposed to each of the individual provider organizations or other end user, who participate through the networks/services) must complete a series of pre-live and ongoing validation steps with other networks including:<br>• Non-production partner test with one other participant<br>• Production connectivity validation – prior to going live a network or service operator must confirm its ability to connect with at least half of the then-live networks, with a report of the results provided to Carequality.<br>• Ongoing production connectivity validation, demonstrating on a quarterly basis that the network/service can continue to connect with other participants.<br><br>Carequality has the right to monitor exchange activity by participants and each participant agrees to cooperate in any monitoring and provide reasonable requested information about its exchange activity to enable the monitoring. | CommonWell has a certification and onboarding process that must be followed by participants wishing to connect to the network. Subsequently, interfaces and data flow are monitored by the network. | DirectTrust requires participants (HISPs, CAs, and RAs) to be accredited to participate in a trust bundle. HISPs applying to participate in a trust bundle must conform to a number of requirements which include ensuring conformance with the DirectTrust Certificate Policy and Profiles and performing bi-directional interoperability testing that requires:<br>• The successful sending and receiving of a message by both the HISP under review and the HISP in the trust bundle;<br>• The receiving HISP must send back an MDN process message to the sending HISP; and<br>• The MDN process message must be successfully received and validated by the sending HISP.<br>The HISP under review must submit a testing address within their production environment that will be used to send and receive test Direct messages with 10 other HISPs that are part of the existing DirectTrust network. Interoperability testing must be successful with 8 of the 10 HISPs and the HISP under review must provide proof of successful testing. The applying HISP's trust anchor is placed in the interoperability testing bundle during the test phase. The 10 HISPs consist of:<br>• 5 HISPs selected from the interoperability HISP pool chosen by the HISP under review.<br>• 5 HISPs randomly selected from the interoperability HISP pool. The trust bundle administrator will execute this selection process.<br>The HISP under review submits all required documentation to the Trust Anchor Approval Committee for review. Every two years after joining the trust bundle a HISP must undertake interoperability testing with one other HISP selected by DirectTrust. |

# TRUST CATEGORY: Accountability

## SUB-CATEGORY: Technical Accountability Mechanism - 2

| eHealth Exchange | NATE | SHIEC | surescripts |
|---|---|---|---|
| All applicants to join the eHealth Exchange must undertake Participant Testing which validates their technology complies with the performance and services specifications used in the eHealth Exchange. Product Testing is an optional program for health IT developers to pursue that verifies their product against a rigorous set of tests. An applicant or participant using a product that has successfully completed product testing may have certain Participant tests waived. Participants are required to have the ability to monitor exchange over their own networks. | NATE has a self-attestation model. | HIOs operate within Regions of their peers, and each HIO retains autonomy, but also stands accountable to honor its commitment to interoperability to its peers. With peers, Regions and National Governance empowered to raise concerns about neighboring partners, all PCDH HIOs remain accountable to one another for their performance. | Certification testing. Contractually-required measures, certification and implementation services, network operations guide, continued customer support and issue resolutions, and audit compliance function. |

# TRUST CATEGORY: Accountability

## SUB-CATEGORY: Network Flow Down

### carequality

Carequality requires participating networks to ensure that a set of standard terms is legally binding on its end users who participate in Carequality through that network. These terms include requirements to:

- Comply with applicable Carequality policies including:
  - Implement and maintain support for at least one Carequality use case.
  - Non-discrimination provisions
  - Comply with the dispute resolution process
  - Only exchange data for permitted purposes
  - Adverse Security Event Reporting
- Comply with applicable law
  - Organizations agree to comply with the HIPAA Business Associate requirements at a minimum, even if the organization is not a covered entity, business associate or governmental entity.
- Reasonably cooperate with issues related to Carequality

### commonwell HEALTH ALLIANCE

CommonWell's agreement with participants requires them to flow down the following requirements to their customers:

- Ensure each end user is properly identified, authenticated, and authorized under applicable law to access the data they are accessing.
- Managing authentication and identity management of end users for access to CommonWell services.
- Comply with applicable law
- Only request access to information for permitted purposes
- Customer shall ensure, and train and obligate its Ends Users to ensure, that patient consents are:
  i. made with full transparency and education;
  ii. made only after the patient has had sufficient time to review educational material;
  iii. commensurate with circumstances for why health information is exchanged;
  iv. not used for discriminatory purposes or as a condition for receiving medical treatment;
  v. consistent with patient expectations; and
  vi. revocable at any time.
- Fraud Detection; Security Breach. Customer must make reasonable efforts to notify the participant of any material security breaches related to the Core Commercial Services promptly after discovery.

### DirectTrust

HISPs must have contractually binding legal agreements with any clients that act as Direct message exchange senders and/or receivers of PHI. Such agreements must include all terms and conditions required in a Business Associate agreement.

# TRUST CATEGORY: Accountability

## SUB-CATEGORY: Network Flow Down - 2

| eHealth Exchange | NATE | SHIEC | surescripts |
|---|---|---|---|
| The DURSA includes a number of provisions that a participant must at a minimum flow down to their end users and their health IT developers.<br>For a participant's end users:<br>• Comply with applicable law<br>• Reasonably cooperate with issues related to the DURSA<br>• Exchange data only for a permitted purpose<br>• Only use data in accordance with the DURSA<br>• Breach notification provisions<br><br>Protect passwords and other security measures<br>For a participant's health IT developer if they use the developer in connection with the participant's eHealth Exchange transactions:<br>• Comply with applicable law<br>• Reasonably cooperate with issues related to the DURSA<br>• Breach notification provisions<br>• Protect privacy and security of data as it is being exchanged | N/A | To the extent that a participant delegates its duties under the agreement to a third party (by contract or otherwise) and such third party will have access to data, that delegation shall be in writing and require the third party, prior to exchanging data with any participants, to agree to the same or substantially similar restrictions and conditions that apply to the participant. The participant is responsible for contractually obligating such third parties to comply with the same or substantially similar restrictions and conditions of the agreement, as are applicable to third parties.<br><br>Participants agrees to flow down the following provisions to end users:<br>• Comply with all Applicable Law;<br>• Report a Breach to the participant and<br>• Refrain from disclosing to any other person any passwords or other security measures issued to the end user by the participant.<br><br>Participant agrees to flow down the following provisions to technology partners:<br>• Comply with Applicable Law;<br>• Protect the privacy and security of any Data to which it has access, including a no record retention provision; and<br>• Report such Breach to the participant. | Participants must have written agreement with their customers that include terms substantially similar to the following effect:<br>• Will only use the network for permitted purposes<br>• Adhere to applicable law<br>• Adhere to Surescripts policies including:<br>  ○ Privacy and security<br>  ○ Background checks<br>  ○ Confidentiality of Surescripts materials<br>• Allow Surescripts or the Aggregator to access, inspect and audit records relating to the use of the network or data. |

# TRUST CATEGORY: Accountability

## SUB-CATEGORY: Enforcement

### carequality

The Steering Committee has authority to suspend or terminate participants. The Steering Committee may terminate participants by giving notice if:

- Applicant is in material breach of any of the terms and conditions of the Carequality Connected Agreement and fails to remedy such breach within 30 days after receiving notice of such breach; or
- Applicant breaches a material provision of this Agreement where such breach is not capable of remedy.

The Steering Committee may suspend participants if:

- Applicant has breached a material provision of the Carequality Connected Agreement and failed to cure such breach within fifteen (15) days, or such other period of time that the Parties have agreed to, of receiving notice of same; or
- There is a substantial likelihood that Applicant's acts or omissions create an immediate threat, or will cause irreparable harm, to another entity, include Carequality or other participants.

### commonwell HEALTH ALLIANCE

The Board of Directors may terminate a participants membership if the participant:

- is in default of payment of an applicable membership fee;
- has breached any material obligation of the CommonWell Bylaws, the Membership Agreement, or other Alliance policies or procedures adopted by the Board of Directors;
- has performed or omitted to perform any other act, which act or omission has been specified in writing from time to time by the Board of Directors as giving rise to termination of membership; provided that such specification by the BOD shall never be retroactively effective; or
- is legally dissolved.

### DirectTrust

The Board of Directors may terminate a participant from inclusion in Trust Anchor Bundle(s) immediately if:

i. that Participant is in violation of the accreditation of trust anchor bundle requirements (whether by reason of its own non-compliance or the non-compliance if its separate CA and/or RA, if any), and

ii. that Participant's continued inclusion in DirectTrust Trust Anchor Bundle(s) while in violation these provisions will jeopardize the integrity of DirectTrust Trust Anchor Bundle(s) or will otherwise be immediately detrimental to other Participants.

DirectTrust shall provide the Participant with written notice of, and sixty (60) days in which to cure, any breach of the Federated Services Agreement (including any breach by Participant's separate CA and/or RA, if any, of the CA/RA Addendum). In the event Participant's inclusion in DirectTrust Trust Anchor Bundle(s) has been terminated under the immediate termination provisions, and Participant subsequently cures its noncompliance within the sixty (60) day cure period, the Participant may be readmitted to the DirectTrust Trust Anchor Bundle(s) by the affirmative vote of a majority (greater than fifty percent (50%)) of the Board of Directors of DirectTrust. A material breach of the Federated Services Agreement that is not cured within sixty (60) days of Participant's receipt of written notice from DirectTrust shall result in termination of the Federated Services Agreement, and Participant's exclusion from DirectTrust Trust Anchor Bundle(s).

# TRUST CATEGORY: Accountability

## SUB-CATEGORY: Enforcement - 2

| eHealth Exchange | NATE | SHIEC | surescripts |
|---|---|---|---|
| The Coordinating Committee has the authority to investigate any complaint and determine whether to suspend and/or terminate a participant for acts or omissions that create an immediate threat or will cause irreparable harm to another party in the eHealth Exchange. If a participant is suspended they have the opportunity to develop a plan of correction for review by the Coordinating Committee. If the Coordinating Committee and participant cannot agree on a plan of correction the Coordinating Committee may submit the dispute to the Dispute Resolution Process or terminate the participant. The Coordinating Committee may reinstate a suspended participant upon successful completion of the participant's corrective action plan or other measures as directed by the Coordinating Committee. | NATE has the sole discretion to remove a participant from the trust bundle due to non-conformance with required policies and processes. If NATE determines a participant present a continuing and material risk to the privacy and security of individual's health information they may be immediately removed from the trust bundle. If there is not a continuing and material risk NATE will inform the participant of the suspension decision including how the participant may appeal the decision. If a participant appeals a suspension or removal the appeal will be heard by all other members of the trust bundle with no quorum required and a simple majority deciding the outcome. | The PCDH Governance Council may terminate a participant with or without cause by giving at least 60 days prior notice to the applicable participant after which time the participant will be terminated. If a material breach of the agreement is discovered the Council may terminate the participant with 30 days notice if the breach cannot be cured. If the material breach can be cured, the Council will provide at least 10 days or longer (if approved by a unanimous vote) to do so. If the breach is not cured in the allowed time period the participant will be terminated. At least one representative from the impacted Region must be present at the meeting where a vote to terminate a participant takes place. If no representative is present the absent representatives from the impacted Region will be given one week to submit their votes in writing. The Council may suspend a participant digital credentials based on a reportable breach, successful security incident, or breach of the agreement which results in a substantial likelihood that a participant's acts or omissions create an immediate threat or will cause irreparable harm to another participant or their end users. The Council may restore the participant's digital credentials if the issue is resolved. Additionally, each participant is a member of a Region. Regional procedures may provide for additional means of accountability and enforcement among its members. | Surescripts' compliance team conducts regularly scheduled and ad-hoc compliance checks as needed on all the Participants on the network. If certified software is determined to be out of compliance with Surescripts' requirements Surescripts may:<br>i. provide written notice to Aggregator of such non-compliance;<br>ii. suspend Services to Aggregator; and<br>iii. work with Aggregator to bring the software back into compliance. If Aggregator fails to respond in a timely manner regarding such non-compliance, Surescripts may decertify Aggregator's software.<br>Notwithstanding the foregoing, Surescripts retains the right to immediately suspend access to the Surescripts network and Services, at its sole discretion, in the event that Surescripts perceives there to be a patient safety concern and if such concern is not adequately resolved to Surescripts' satisfaction, to decertify the software. Surescripts may prohibit the use of the Surescripts network on behalf of any participant whose version of the Aggregator software is not currently certified by Surescripts. |

# TRUST CATEGORY: Accountability

## SUB-CATEGORY: Dispute Resolution

| carequality | commonwell HEALTH ALLIANCE | DirectTrust |
|---|---|---|
| Participants agree to participate in Carequality's mandatory, non-binding dispute resolution process. Participation in the dispute resolution process is mandatory but the dispute resolution process preserves participants' right to seek remedies in the courts if the dispute is not resolved through the process. The non-binding aspect is necessary for governmental participants that are prevented, by law, from agreeing to binding arbitration or other binding forms of dispute resolution. The first step in the process is an informal conference between the participants involved in the dispute to attempt to resolve it in good faith. If the dispute is not resolved, a Dispute Resolution Subcommittee of the Steering Committee hears the dispute and can develop a recommended resolution which is reviewed by the Steering Committee. The Steering Committee can issue a decision based on this information or send the dispute back to the Subcommittee for further study or information. Any party of the dispute can appeal the decision of the Steering Committee to the Carequality Advisory Council, which will make a final resolution on the dispute. | Good faith dispute resolution process. A dispute notice must be sent by the originating party, the receiving party has 15 days to respond. Within 30 days of delivery of the dispute notice the parties must meet and attempt to resolve the dispute. If a resolution is not reached through these negotiations the dispute can move to federal or state court of the relevant jurisdiction in the state of Delaware. | Participants shall attempt to resolve the dispute through good-faith negotiations. If negotiations fail to achieve a satisfactory resolution within fifteen (15) days after either party provides written notice of the dispute, then binding arbitration shall be used to resolve the dispute, unless one of the Participants is a government entity. In lieu of arbitration, a government entity shall have the right to proceed to court. Any Participant with an interest in the dispute shall have the right to intervene as a party. The parties to a binding arbitration shall mutually select an arbitrator. If the parties fail to select an arbitrator, then the DirectTrust Board of Directors shall select an arbitrator that they believe can fairly and impartially resolve the dispute. Arbitration will occur at a place mutually selected by the parties. If a place cannot be mutually agreed to, then the parties will arbitrate the dispute in Washington, D.C. Absent other agreement among the parties, the arbitration shall be governed by the commercial arbitration rules and procedures of the American Arbitration Association. The decision of the arbitrator shall be final and binding for purposes of the Federated Services Agreement. |

# TRUST CATEGORY: Accountability

## SUB-CATEGORY: Dispute Resolution - 2

| eHealth Exchange | NATE | SHIEC | surescripts |
|---|---|---|---|
| Participants agree to participate in the eHealth Exchange's mandatory, non-binding dispute resolution process. Participation in the dispute resolution process is mandatory but the dispute resolution process preserves participants' right to seek remedies in the courts if the dispute is not resolved through the process. This is necessary for governmental Participants which are prevented, by law, from agreeing to binding arbitration or other binding forms of dispute resolution. The first step in the process is an informal conference between the participants involved in the dispute to attempt to resolve it in good faith. If the dispute is not resolved, the Dispute Resolution Subcommittee (Subcommittee) of the Coordinating Committee hears the dispute and can develop an appropriate and equitable resolution. If requested by any participant involved in the dispute, the Coordinating Committee can review the Subcommittee's recommendation and issue its own resolution. | N/A | If there is a dispute between participants arising in relation to the agreement, a participant may give written notice of the dispute to each participant that may be involved in the dispute, and each organization involved in the dispute must then designate an individual to confer in good faith in an attempt to resolve the dispute. The PCDH Governance Council may adopt a policy and procedure to assist participants in resolving disputes in an informal manner. If a dispute cannot be resolved informally the governing law will be the law of the state of the principal business of the participant responding to the dispute. | In the event of a Dispute, the parties shall meet and confer in good faith to resolve such dispute. In the event such efforts do not resolve the Dispute within fifteen (15) days from the date the dispute arises, either party may demand arbitration administered and conducted in Washington, D.C., by the American Arbitration Association, before one (1) arbitrator, under its Commercial Arbitration Rules, such arbitration to be final, conclusive, and binding. |

# TRUST CATEGORY: Other

## SUB-CATEGORY: Fees for Data Exchange Among Participants

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| Any policy around fees charged to other participants is defined in each use case Implementation Guide. Under the Query-Based Document Exchange Implementation Guide the policy varies by permitted purpose. Participants may not charge one another fees for queries or responses for treatment purposes. Participants are allowed to charge fees for queries or responses for other permitted purposes. | Participants are not allowed to charge fees to exchange through CommonWell with other participants, for treatment and patient direct access use cases. | Accredited HISPs are not allowed to charge one another to transmit or receive a basic Direct messages. | eHealth Exchange does not have a policy permitting or prohibiting participants from charging fees for transactions with other participants. | NATE does not have a policy permitting or prohibiting participants from charging fees for transactions with other participants. | SHIEC does not have a policy permitting or prohibiting participants from charging fees for transactions with other participants. | There are applicable fees, however fee information has been omitted from shared documents. |

# TRUST CATEGORY: Other

## SUB-CATEGORY: Encryption

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| TLS | TLS/SSL | S/MIME, SMTP, for last mile delivery between an edge client and a HISP SSL/TLS or an equivalent industry standard must be used. | TLS | Participants must encrypt all edge protocol communications (last mile exchange). | All PCDH interfaces must be established using methods consistent with the definition of "Encryption" in the HITECH Act. HIOs work together within regions, and between regions to establish the most appropriate encrypted connection methods. At a minimum, members agree to comply with the applicable HIPAA/HITECH standards for securing data. Specs will be formalized as needed by PCDH Regions and the Governance Council. | Encryption-related services, including network level encryption which is employed by Surescripts for all transactions through the Surescripts network and optional payload encryption for SCRIPT transactions, which must be determined between the Participants to a transaction and for which they are solely responsible. If Aggregator decides to utilize payload encryption, Aggregator must notify Surescripts in advance in writing and must be certified by Surescripts to utilize the Surescripts custom point-to-point transaction. |

# TRUST CATEGORY: Other

## SUB-CATEGORY: Participant API Documentation Requirement

| carequality | commonwell HEALTH ALLIANCE | DirectTrust | eHealth Exchange | NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE | SHIEC Strategic Health Information Exchange Collaborative | surescripts |
|---|---|---|---|---|---|---|
| There are no specific API documentation standards required of participants. | There are no specific API documentation standards required of participants. | There are no specific API documentation standards required of participants. | There are no specific API documentation standards required of participants. | There are no specific API documentation standards required of participants. | There are no specific API documentation standards required of participants. | There are no specific API documentation standards required of participants. |