Smart Health Network

NETWORK RULES

VERSION 1.0

Effective date: as stated in the applicable adoption notice.

Executive Summary

Healthcare organizations have digitized their own systems, but the work between them still too often depends on separate connections, repeated checks, portals and phone calls. Smart Health Network brings people, providers, payers, and their partners together through shared, neutral infrastructure and common rules. Participants can connect once and reuse trust and connectivity across relationships and use cases, reducing repeated contracting, verification and integration work. The primary exchange path uses Participant Gateways and a Hub that routes encrypted Messages without reading their content. Each Participant retains responsibility for its own legal authority and substantive decisions.

Prior authorization is the starting point. The initial Transaction Catalog designates 17 Transaction Types as Open Access. SHN charges no fees for Network participation, connection, Network Trust Services or Open Access Transactions within their designated scope. Production availability and each Participant's activation are established separately. Individuals can access information about Network activity involving their data and exercise their applicable rights through supported applications, including Participant and third-party applications.

Smart Health Network PBC ("SHN") is a public benefit corporation. The Governance Council's reserved governance and approval rights protect the Network's neutrality and public purpose, and the independent Data Rights Trust exercises its enumerated powers to protect Individual Rights. These Network Rules establish the responsibilities of SHN and Participants and the common protections governing Open Access, privacy, security, information use and accountability. Changes follow Section 3.2 and the Governing Instruments, including the approvals required to change protected rights.

Finding your way through the Rules

Section 1: Definitions.
Section 2: Network Infrastructure and SHN Services.
Section 3: Governance of the Network.
Section 4: Participation in the Network.
Section 5: Individual Rights and Member Services.
Section 6: Authorized Interactions and Transaction Framework.
Section 7: Network Security.
Exhibit A: Open Access and Fee Structure.
Exhibit B: Initial Transaction Catalog.
Exhibit C: Base Service Level Agreement.
Initial Transaction Specification: Prior Authorization, Version 1.0.

1. DEFINITIONS.

Capitalized terms used in these Network Rules have the meanings set forth in this Section 1 or the meanings set forth in the Network Participation Agreement.

1.1 "Additional Services" means separately elected services provided by SHN to or for the benefit of a Participant beyond functions required to be included under these Network Rules and Exhibit A. Authorized categories include Enhanced Support, Gateway Management, Network Management, Network Intelligence, and Network Orchestration. Their scope, responsibilities, and fees are established in a Service Order. A function does not become an Additional Service merely because it is bundled with or delivered through one.

1.2 "**API**" means application programming interface.

1.3 "**Applicant**" means an individual or entity that is seeking to become a Participant but has not yet been recognized as a Participant by SHN.

1.4 "Audit Log" means the attributable record of Hub Transactions and related events observed by the Hub, maintained under Sections 2.3 and 7.8.

1.5 "Authorized Actor" means an individual, entity, application, bot, or automated agent designated by a Participant or Member to act on its behalf within an established scope of authority. A Business Associate may be an Authorized Actor, but that status alone does not establish authority for a particular action. Member designations are governed by the Member Terms and Section 5.

1.6 "Authorized Third Party Service" means an independently provided service supplied by a qualified third party to Participants or Members using permitted Network capabilities. It is distinct from services undertaken by SHN. A provider may embed an SHN Member Service while remaining responsible for its own functions.

1.7 "**Authorized Third Party Service Provider**" means a third party service provider that provides Authorized Third Party Services.

1.8 "Authorized User" means a natural person designated by a Participant to access or use a Participant Gateway or another SHN-provided interface or service on the Participant's behalf.

1.9 "**Business Associate**" has the meaning set forth at 45 C.F.R. § 160.103.

1.10 "Business Day" means any day from Monday through Friday other than a United States federal holiday, unless an applicable Jurisdiction Schedule expressly provides otherwise.

1.11 "**CMS**" means the Centers for Medicare & Medicaid Services.

1.12 "Data Processing Agreement" means an applicable agreement addressing data processing in the relevant service capacity, including a Business Associate Agreement to the extent SHN acts as a Business Associate and any other required processing, confidentiality, or transfer terms.

1.13 "Data Requestor" means a person or service requesting data within a role recognized by the applicable Transaction Specification or exercising an applicable right under Section 5, including a Participant, Member, Individual, lawfully authorized representative, or Authorized Actor, as applicable. This definition does not itself establish Participant or Member status or authority to obtain or disclose information.

1.14 "Data Rights Trust" means the independent patient-data-rights body exercising the enumerated determination, consent, certified-finding, governance-share and other rights assigned to it under Section 3.1(c) and its Governing Instruments.

1.15 "Enhanced Support" means separately purchased assistance or coverage beyond support included in the applicable Network function or operating service. It may include additional contact hours, response commitments, architecture or release reviews, and integration, migration, training, or testing assistance. Required qualification support, common security fixes, and other included functions remain included.

1.16 "**Gateway**" means either a Member Gateway or a Participant Gateway.

1.17 "**Governance Council**" means a separate governance body that is responsible for overseeing the Network in accordance with Section 3.1(b).

1.18 "Gateway Management" means SHN's operation of a Participant Gateway under a Service Order, including the deployment, configuration, maintenance, monitoring, recovery, and support responsibilities specified there. "Managed Gateway" describes this operating arrangement; hosting location alone does not establish operating responsibility.

1.19 "**Governing Instruments**" means, in the case of Smart Health Network PBC, its charter and bylaws, in the case of the Governance Council, its trust agreement and bylaws, and in the case of the Data Rights Trust, its trust agreement and bylaws.

1.20 "**Health Care Provider**" means any individual or entity that furnishes, bills, or is paid for health care in the normal course of business.

1.21 "**Health Plan**" means an individual or group plan, program, issuer, or other arrangement that provides health benefits or pays the cost of medical care. In the United States, the term "Health Plan" includes the plans listed under the definition of "health plan" at 45 C.F.R. § 160.103.

1.22 "**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, as amended from time to time, and the regulations issued under 45 C.F.R. Parts 160, 162, and 164.

1.23 "**Hub**" means the SHN software and services that perform the functions described in Section 2.2(a).

1.24 "Hub Audit Log and Retention Specification" or **"Retention Specification"** means the single versioned specification maintained under Section 7.8(c) for the Hub Audit Log and, separately, temporary encrypted Message transport state.

1.25 "**Hub Transaction**" means a Transaction that is routed through the Hub.

1.26 "**Identifiable Individual Data**" means Individual Data that is Personal Data.

1.27 **"Individual"** means a natural person about whom data is transmitted, processed, maintained, or otherwise handled in connection with the Network, whether or not that person is a Member.

1.28 "**Individual Data**" means data about one or more Individuals. Individual Data includes both de-identified data and Identifiable Individual Data.

1.29 **"Jurisdiction Schedule"** means an instrument, adopted as a Rule Document under Section 3.2, that supplements these Network Rules for Network activity in an identified jurisdiction as described in Section 6.8.

1.30 **"Member"** means an Individual who has established a direct service relationship with SHN under the Member Terms to use or receive Member Services. An Individual does not become a Member solely because Individual Data about that Individual is processed or exchanged through the Network.

1.31 **"Member Gateway"** means software supporting a Member's interaction with the Network, including the functions described in Section 2.2(c). The Member Gateway is a technical component and does not require Member Services to be delivered through a standalone SHN application.

1.32 "**Member Service**" means a service that SHN provides to or on behalf of a Member. For example, a "Member Service" may consist of transmitting data on a Member's behalf between such Member and a Participant or providing notice to a Member relating to the status of such Member's claim or prior authorization request.

1.33 **"Member Terms"** means the terms governing the direct service relationship between SHN and a Member, including the Member's use or receipt of Member Services and SHN's processing of Individual Data in connection with those services.

1.34 **"Message"** means the substantive content communicated in a Network Transaction, regardless of its format, encryption, or Qualified Transaction Path. Message content may include a request, source response, clinical information, or remittance advice. Encryption requirements for Hub Transactions are set forth in Sections 2.3 and 7.3.

1.35 **"Metadata"** means information about a Network Transaction and its handling, excluding Message content or a reproduction of substantive information contained in a Message. It may include transaction and endpoint identifiers, Transaction Type, a scoped PCI, and the time and nature of an observed transport event. Metadata remains subject to applicable privacy, security, and information-use restrictions.

1.36 **"Network"** means the common trust and interaction framework established by these Network Rules, the Network Participation Agreements, and Member Terms, together with the Network Infrastructure and qualified arrangements supporting that framework. Participants' and third parties' unrelated systems and activities do not become part of the Network merely through connection or participation.

1.37 "Network Accountability Office" means the function within SHN responsible for complaints, investigations, development of the factual record, findings and recommendations, and follow-up under Section 3.3.

1.38 "**Network Directory**" means a publicly available compilation of information about each Participant, which may include certain information available in a Participant Profile.

1.39 "**Network Exchange Service**" means a service provided by SHN involving the routing of data through the Hub among Participants and/or Members.

1.40 "**Network Infrastructure**" means the technical systems and components that SHN provides, maintains, or recognizes as part of the common infrastructure supporting Network participation or Network Transactions, including the Hub, the Member Gateway, the Participant Gateway, the Network Directory, registries related to Individual decisions, and other systems designated by SHN as part of such common infrastructure. For the avoidance of doubt, Network Infrastructure does not include (i) a Qualified Transaction Path other than the Hub, (ii) a Participant's or third party's systems merely because they connect to or are used in connection with the Network, or (iii) software or systems used solely to provide Additional Services or Authorized Third Party Services.

1.41 "Network Intelligence" means software or a service producing an additional authorized analytical or derived result for a Participant, such as insights, benchmarks, trends, forecasts, or recommendations. Its scope shall identify permitted inputs, processing, outputs, recipients, and retention. It shall not disclose information identifying and evaluating another Participant on a performance metric without that Participant's consent or reprice information or work already included or purchased.

1.42 "Network Management" means software or a service applying a Participant's additional requirements and operating workflows across its elected external relationships, services, and paths, including qualified paths outside SHN-Operated Infrastructure. It may provide a consolidated operating view, identify relationships affected by change, reuse evidence, initiate permitted reassessment or retesting, and manage remediation and exceptions. Required common trust and responsibility resolution remain included.

1.43 "Network Orchestration" means separately commissioned coordination of authorized actions and dependencies across Participants or Members toward an identified objective beyond the work completed by the underlying individual exchanges. It may obtain information from multiple sources, coordinate responses, and direct authorized actions or notifications. Source decisions remain attributable to their responsible parties, and required handling of an Open Access Transaction remains included.

1.44 "**Network Participation Agreement**" means an agreement between SHN and an individual or entity that allows such individual or entity to participate in the Network, inclusive of any Data Processing Agreement between SHN and the Participant. For the avoidance of doubt, Members do not sign Network Participation Agreements, unless they are separately seeking to become Participants.

1.45 "Network Security Incident" means an actual or reasonably suspected unauthorized acquisition, access, use, disclosure, alteration, or destruction of information, compromise of keys or credentials, or material compromise of system integrity or availability affecting Network Transactions, Network Trust Services, Member Services, or other services provided under these Network Rules. It includes affected components of non-Hub Qualified Transaction Paths to the extent relevant to those functions. Routine unsuccessful attempts that do not compromise systems or information are excluded unless they indicate a material threat requiring action. Whether an incident is reportable as a breach under applicable Privacy Law is a separate determination and does not delay reporting required by these Network Rules.

1.46 "Network Transaction" means an exchange identified as conducted under an accepted Transaction Specification, through a Qualified Transaction Path, within the applicable parties' activated roles and scope. Participants may accept recurring exchanges in advance under specified conditions; Member participation is established under the Member Terms and supported service scope. Use of a qualified connection alone does not make an exchange a Network Transaction. Rejection, failure, or breach does not remove an identified Network Transaction from the applicable requirements.

1.47 "Network Trust Services" means the services that SHN performs to (i) establish and maintain the identity and standing of Applicants and Participants; (ii) maintain, verify, or resolve against qualified sources information concerning Participants and their relationships, responsibility, capabilities, authorized actors and services, endpoints, Qualified Transaction Paths, and applicable scope and current status; and (iii) make that information available to entitled persons and services to facilitate Network participation and supported Network Transactions. These services include maintenance of Participant Profiles and the Network Directory and mechanisms for updating, challenging, and correcting relevant information. Common trust and responsibility resolution identifies or verifies the parties, roles, authority, services and destinations relevant to a supported interaction. Substantive discovery, reconciliation, computation and coordination of a business process may be separately commissioned within an authorized service category. Required verification of a claimed role, authority or destination remains included.

1.48 "**NIST**" means the United States National Institute of Standards and Technology.

1.49 "**Participant**" means an individual or entity that is a party to an executed Network Participation Agreement with SHN that is in effect.

1.50 "Participant Advisory Council" means a council that represents the interests of Participants with respect to the Network in accordance with Section 3.1(d).

1.51 "Participant Gateway" means software deployed by or on behalf of a Participant that implements the Participant's trusted digital boundary for supported interactions, including the functions described in Section 2.2(b), and satisfies applicable Network qualification requirements. A Participant Gateway may use SHN-provided software or another qualified implementation. Software providing Additional Services is not part of the Participant Gateway solely because it is integrated with or deployed alongside the Participant Gateway.

1.52 "**Participant Profile**" means a maintained record of information concerning a Participant's participation in the Network, including its identifying information, effective date of participation, designated points of contact, roles and capabilities, endpoints, applicable deployment models and operators, Authorized Actors, Transaction Schedule, applicable Qualified Transaction Paths, and qualification and activation status for its elected scope. A Participant Profile may incorporate information by reference to other maintained records.

1.53 **"Patient Correlation Identifier"** or "PCI" means an opaque identifier assigned to an Individual for correlation within a defined Network scope. A PCI shall not be derived from identifying information about the Individual or reveal the Individual's identity without access to a separately maintained, access-controlled mapping.

1.54 "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular natural person. Personal Data includes, but is not limited to, PHI.

1.55 **"PHI"** or **"Protected Health Information"** has the meaning set forth at 45 C.F.R. § 160.103.

1.56 "**Privacy Law**" means any law or regulation governing the processing, disclosure, privacy, or security of Individual Data. In the United States, "Privacy Law" includes, but is not limited to, HIPAA, the federal substance use disorder confidentiality regulation (42 C.F.R. Part 2), and state laws governing the privacy of health care records. Outside of the United States, "Privacy Law" includes, but is not limited to, the European Union General Data Protection Regulation, the United Kingdom General Data Protection Regulation, South Africa's Protection of Personal Information Act, Brazil's General Personal Data Protection Law, and Singapore's Personal Data Protection Act.

1.57 "**Public Health Authority**" means a government agency or authority, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

1.58 **"Qualified Transaction Path"** means a technical and operating path recognized by SHN as satisfying the applicable requirements for an identified Network interaction, role, implementation, and scope, including geography where relevant. It may use the Hub, a direct API, another network, or another accepted means of execution. Qualification applies to the specified interaction and does not qualify every exchange carried over the same connection or make SHN the operator of the path.

1.59 **"Rule Documents"** means Exhibit A (Open Access and Fee Structure), Exhibit B (Initial Transaction Catalog, as subsequently maintained and published under these Network Rules), Exhibit C (Base Service Level Agreement), the Hub Audit Log and Retention Specification, and each Jurisdiction Schedule. References to these Network Rules include the Rule Documents.

1.60 **"Service Order"** means an agreement between SHN and a Participant or another authorized purchaser establishing separately purchased Additional Services or an approved paid Transaction Type, including the purchased scope, beneficiary Participants where applicable,

operating and payment responsibilities, fees, service terms, and applicable transition arrangements.

1.61 "**SHN**" means Smart Health Network PBC, a Delaware public benefit corporation that operates the Network.

1.62 "**SHN-Operated Infrastructure**" means the software, systems, and technical infrastructure operated by or on behalf of SHN to perform its obligations or provide services under these Network Rules, Member Terms, or an applicable Service Order, including the Hub, infrastructure supporting Network Trust Services and Member Services, and infrastructure supporting Additional Services. A Participant Gateway is SHN-Operated Infrastructure only to the extent SHN undertakes responsibility for its operation under an applicable Service Order.

1.63 "**Six Commitments**" means the six core requirements related to the operation of the Hub which are set forth in Section 2.3.

1.64 **"Transaction"** means a transmission, request, response, or other exchange of data by or between one or more Participants, Members, or persons or services authorized to act on their behalf. A Transaction may concern Individual Data about an Individual who is not a Member.

1.65 **"Transaction Catalog"** means the maintained registry of Transaction Types, their scope, geographic coverage, availability, and Open Access or paid designation. Exhibit B contains the initial Catalog; subsequent versions are maintained and published under Section 6 and Exhibit A. Listing does not itself establish acceptance, production activation, payment obligations, or authority to access or disclose information.

1.66 "**Transaction Schedule**" means the maintained record of the Transaction Types and corresponding roles and scope that a Participant has accepted under the Network participation framework, including the applicable Transaction Specification versions or accepted compatibility rules. Acceptance does not itself establish production activation.

1.67 **"Transaction Specification"** means the accepted technical and operational requirements for a Transaction Type, including its purpose, roles, supported actions, representations, required controls, applicable authority and consent conditions, response meanings, evidence, correlation, failure and recovery behavior, and implementation requirements. A Transaction Specification may not alter the Six Commitments, impose new fees, or otherwise conflict with these Network Rules.

1.68 **"Transaction Type"** means an identified category of Transactions with a defined purpose and supported interaction pattern, as described in the Transaction Catalog and applicable Transaction Specifications.

2. NETWORK INFRASTRUCTURE AND SHN SERVICES.

2.1 Overview of SHN Services.

Participation, Network Trust Services and designated Open Access exchanges are provided without SHN fees as specified in Exhibit A. Additional Services are optional and separately agreed.

(a) SHN shall operate the Hub and other SHN-Operated Infrastructure and provide Network Exchange Services in accordance with these Network Rules. Participants and other operators remain responsible for the functions assigned to them under the applicable operating arrangements. SHN's recognition of a Qualified Transaction Path does not itself constitute an undertaking to operate that path. Participants retain responsibility for their substantive clinical, coverage, payment, and other business decisions and underlying relationships. SHN remains responsible for the functions it undertakes; performing those functions does not transfer those substantive decisions to SHN. Participation, use of Network Trust Services, or performance of a Network Transaction does not, by itself, amend underlying counterparty relationships or create a direct contractual claim by one Participant against another under these Network Rules. Additional direct contractual reliance rights, remedies, or indemnities require express acceptance in an applicable agreement identifying their scope and limitations. This provision does not limit applicable law, independently applicable agreements, Individual rights, SHN's enforcement authority, or responsibility for functions expressly undertaken.

(b) SHN shall provide the Network Trust Services with respect to all Participants, regardless of whether such Participants engage in Network Transactions, deploy a Participant Gateway, or purchase Additional Services. In performing Network Trust Services, SHN shall preserve the source, scope, and currency of evidence; perform the verification required for the applicable function; and make material changes, expirations, revocations, and corrections available to affected parties within the applicable operating requirements. Where evidence is insufficient or unresolved, SHN shall identify that limitation and the scope of any verification actually completed. SHN shall maintain published operating requirements identifying the verification standard, evidence currency, material-change propagation, correction process, and handling of unavailable, conflicting, expired, or revoked evidence for the relevant trust function. Relying parties shall perform the checks assigned to them.

(c) SHN may provide Additional Services to Participants under an applicable Service Order, provided that (i) SHN shall not require a Participant to purchase Additional Services as a condition of becoming a Participant in the Network or as a condition of remaining a Participant in the Network; and (ii) any processing or disclosure of information for Additional Services must have the applicable authority and comply with these Network Rules.

(d) SHN may provide Member Services under Member Terms. Before launch, SHN shall establish the applicable Member Terms, supported functions and source coverage, information-handling and complaint arrangements, continuity, and the safeguards and processing instruments required for its actual capacity. Once undertaken, those services shall be provided in accordance with the applicable Member Terms and these Network Rules.

2.2 **Operation of the Network Infrastructure**. SHN shall operate the Hub and other components for which it undertakes operating responsibility. Participants may operate their own components or appoint qualified operators, as provided in these Network Rules and applicable

operating arrangements. SHN may update, replace or retire components it operates, subject to applicable notice, qualification and continuity requirements and protection of included functions and existing commitments. Such a change does not itself authorize withdrawal of a supported Transaction Type or reduction of protected scope.

(a) **The Hub.** The Hub routes Hub Transactions among Gateways, performs the controls assigned to it, and maintains attributable, auditable records of the transport events it observes. The Hub shall operate in accordance with the Six Commitments and shall not have access to Message-decryption keys or decrypt Message content.

(b) **The Participant Gateway.** The Participant Gateway provides the Participant's trusted digital boundary for supported interactions within its elected scope. It establishes relevant counterparty and trust context, applies local policy and required authority checks, routes Transactions to the appropriate system or service, and preserves evidence of its actions and observations. It may support Hub Transactions and other Qualified Transaction Paths. For Hub Transactions, it shall encrypt outbound Message content before transmission to the Hub and decrypt inbound Message content only within the applicable authority. Each Participant may choose among the following models for deployment of the Participant Gateway:

(i) ***Participant-Operated Gateway.*** The Participant operates the Participant Gateway using its own infrastructure or a hosting provider.

(ii) ***Appointed-Operator Gateway.*** A qualified operator operates the Participant Gateway on the Participant's behalf, including through a shared deployment that preserves each Participant's identity, authority, and information boundaries.

(iii) ***Managed Gateway.*** SHN operates the Participant Gateway on the Participant's behalf under an applicable Service Order.

(iv) ***No Participant Gateway.*** The Participant uses Network Trust Services and, where activated, Qualified Transaction Paths that do not require a Participant Gateway.

(c) **The Member Gateway.** The Member Gateway supports a Member's access to entitled information and exercise of supported rights and actions under the Member Terms and applicable Transaction Specifications. For Hub Transactions, it shall encrypt outbound Message content before transmission to the Hub and decrypt inbound Message content only within the Member's applicable authority and entitlement. Member Services may also use authorized source events from Qualified Transaction Paths other than the Hub.

2.3 Six Commitments. SHN shall ensure that the Hub operates in accordance with the following principles:

(a) **Message Blind Routing.** The Hub shall route Hub Transactions without being able to read their Messages. All Messages shall be encrypted by the applicable Gateway before transmission to the Hub and shall remain encrypted while handled by the Hub.

(b) **Non-Aggregation.** The Hub shall not aggregate Message content or maintain Messages as a repository of substantive data. The Hub may temporarily retain

encrypted Messages solely as necessary for routing, delivery, retry, and recovery, subject to defined retention limits and deletion requirements. The Hub shall maintain Metadata concerning Hub Transactions in accordance with these Network Rules, but such Metadata shall not include Message content or reproduce substantive information contained in a Message. For example:

(i) If the Hub routes a prior authorization request from one Participant to another Participant with respect to a particular Individual, the Metadata maintained by the Hub may include the time and date of such Transaction, the Participants to such Transaction, the Transaction Type, and the PCI of the applicable Individual, but the Hub shall not maintain any information about the content of the Message, such as the service for which prior authorization is being sought or the Individual's name or address.

(ii) If the Hub is used to route a Hub Transaction carrying a Message relating to a particular item or service from a Participant to a Member Gateway, the Metadata maintained by the Hub may include the time and date of such Transaction, the Participant who has provided the Message to the Member, and the Member's PCI, but not the content of the information disclosed to the Member (including the item or service that is included in such Message) or the Individual's name or address.

(c) **No Backdoor.** The Hub shall not possess or have direct or indirect access to keys or other capabilities that enable it to decrypt Messages. SHN shall maintain separation of key custody, privileged access, and administration sufficient to prevent its operation of a Gateway or another service from enabling the Hub to decrypt Messages.

(d) **Authorization for Every Transaction.** A Hub Transaction may proceed only within a Transaction Type listed in the Transaction Catalog and the applicable parties' accepted and activated roles and scope, under the applicable Transaction Specification. Required actor authority, Individual consent, and other applicable authorization conditions shall be satisfied. Participants and other responsible parties shall establish the lawful basis for their actions under applicable Privacy Law. The Hub shall enforce the authorization controls assigned to it by these Network Rules and the applicable Transaction Specification; controls requiring access to Message content shall be performed by the responsible Gateway or other authorized service.

(e) **Record of Every Transaction.** The Hub shall maintain an attributable, tamper-evident Audit Log of every Hub Transaction, including rejection, failure, and recovery events it observes. Recorded entries shall be protected against unauthorized alteration or deletion. Corrections shall be recorded as linked subsequent entries that preserve the original record during its applicable retention period. Retention and authorized deletion shall comply with these Network Rules and applicable law.

(f) **Individual Rights.** Each Individual shall have the right to access Metadata maintained by the Hub concerning that Individual, subject to appropriate identity verification and applicable law. SHN shall provide a usable means of exercising that right. Information shall be presented in a form that protects other persons' information and security credentials while preserving the Individual's entitled visibility into the relevant Network activity. Any withholding or

redaction shall be limited to what is necessary to comply with applicable law or protect such information or credentials.

2.4 **Enforcement of Six Commitments**. A Participant, an affected Individual or lawfully authorized representative, the Governance Council, or the Data Rights Trust may provide SHN with written notice describing an alleged material violation of one or more of the Six Commitments. An adequately described complaint received by the Network Accountability Office constitutes notice to SHN for this purpose. Upon receipt or SHN's own discovery of a credible indication of a material violation, SHN shall promptly investigate and take appropriate measures to contain any ongoing violation and mitigate its effects. The matter shall also be referred to the Network Accountability Office for investigation and potential action in accordance with Section 3.3. If SHN has materially violated a Six Commitment and fails to cure that violation within thirty (30) days after receipt of such notice, any Participant materially affected by the violation may terminate its Network Participation Agreement immediately upon written notice, without penalty or the notice period otherwise required under that agreement. Such termination shall not discharge obligations accrued before termination or obligations that expressly survive termination. This provision does not limit other rights or remedies available under the applicable governing instruments, agreements, or law.

2.5 **Participant Gateway Configuration**. A Participant may configure and operate its Participant Gateway, directly or through its appointed operator, within the scope of its qualified implementation and applicable operating arrangements, subject to the following requirements:

(a) **Participant-Configurable Elements**. A Participant may configure supported settings without SHN's prior approval, including: (i) its Authorized Users of the Participant Gateway and their access permissions and credentials; (ii) internal routing rules and supported destinations; (iii) local policies consistent with applicable Network requirements; and (iv) alert thresholds and notification preferences. Such configuration shall not disable required controls, expand the Participant's activated scope, or impair required evidence or reporting.

(b) **Elements Requiring SHN Approval.** A Participant shall obtain SHN's prior written approval before making a change outside the parameters of its qualified implementation that materially affects: (i) encryption or key exchange for Hub Transactions; (ii) required Metadata or Audit Log interfaces; (iii) authentication or authorization controls used for Network Transactions; or (iv) controls necessary to preserve the Six Commitments. SHN shall not unreasonably withhold or delay approval.

(c) **Prohibited Modifications and Uses**. A Participant shall not modify or configure its Participant Gateway to: (i) transmit unencrypted Message content to the Hub or enable the Hub to decrypt Messages; (ii) bypass required authentication, authorization, consent, security, or evidence controls; (iii) permit unauthorized access to or alteration of Hub routing or Audit Log records; or (iv) initiate or process Network Transactions outside its accepted and activated roles and scope. Storage, logging, and processing of Message content at the Participant Gateway shall comply with the applicable authority, purpose, access, security, and retention requirements. Qualification of a Participant Gateway does not bring every other use of that Gateway within the Network Transaction framework.

(d) **Version Control and Updates**. For SHN-provided Participant Gateway software, SHN shall identify supported versions and provide advance written notice of required updates, the reasons for them, and the applicable implementation deadline. For an ordinary required update, the deadline shall be no earlier than ninety (90) days after release, with at least thirty (30) days' advance written notice. For a security update addressing an active vulnerability, SHN may require earlier implementation, with as much notice as practicable and no fewer than seventy-two (72) hours to implement unless an emergency requires a shorter period. Participants using another qualified implementation shall maintain conformance with applicable Network requirements and implement necessary remediation within the applicable notified period. Where SHN operates the Participant Gateway, SHN shall perform the updates within its operating responsibility. SHN may suspend affected Network activity in accordance with Section 4.4 if an unsupported or nonconforming implementation poses a material security risk to the Network.

2.6 **Maintenance of Registries**. SHN may maintain, or provide resolution services against, registries and other maintained records supporting Network participation and Transactions, including:

(a) **Participants and Standing.** Participant identity, participation status, Participant Profiles, designated contacts, and information used to maintain the Network Directory.

(b) **Relationships and Authority.** Relationships among Participants and other relevant persons or services, including responsibility for supported functions, Authorized Actor designations, operator appointments, and their applicable scope, effective periods, and current status.

(c) **Capabilities, Services, and Endpoints.** Supported capabilities and services, the Participants or operators responsible for them, available endpoints, and applicable discovery and access restrictions.

(d) **Transaction Scope and Qualification.** Transaction Types and Specifications, Participant Transaction Schedules, Qualified Transaction Paths, and qualification and activation records for the applicable roles, implementations, and scope.

(e) **Individual Decisions.** Individual consent decisions and other applicable permissions or instructions, including their scope, effective periods, current status, and any withdrawal or supersession.

(f) **Identifier Correlation.** Associations between PCIs and Individual identifiers within the applicable correlation scope.

2.7 **Transparency and SHN Use of Data**.

(a) **Network Directory and Discovery.** SHN may publish information from Participant Profiles designated for public discovery under these Network Rules, including Participant identifying information and publicly available capabilities, endpoints, and Transaction Types. SHN may make other Participant Profile information available to

Participants, their Authorized Actors, Individuals, and other entitled persons or services to the extent necessary for authorized Network participation or Transactions. Nonpublic endpoints, relationships, capabilities, credentials, and other restricted information shall remain subject to applicable access and disclosure controls.

(b) **Network Utilization Reports.** SHN may publish aggregate reports concerning Network participation and utilization, using information it is authorized to process for that purpose. Such reports may include the number and geographic distribution of Participants, the number of Participants by category, the number of Network Transactions in total and by Transaction Type, and aggregate counts and geographic distribution of Individuals whose data is exchanged through the Network. Reports shall identify their relevant scope and period and distinguish observed activity from estimates. SHN shall apply appropriate aggregation, suppression, or other safeguards to prevent reports from identifying Individuals or revealing information about identifiable Individuals. SHN shall not publish information prohibited from disclosure by applicable Privacy Law or information that identifies a Participant and evaluates that Participant on a performance metric without its consent. Additional categories of publicly reported information shall be described in these Network Rules through the applicable amendment process before publication.

(c) **Limits on Information Use.**

(i) **Purpose and Use Limits.** SHN shall access, retain, combine, analyze and disclose information only for purposes authorized under the applicable service arrangement, these Network Rules and applicable law. Participation, inclusion in a Participant Profile or use of Network services grants no general right to use Participant or Individual information for unrelated purposes. Authority for one service does not authorize another service, unrelated secondary use or reusable model training. Aggregation, anonymization or de-identification does not supply authority to process the underlying information. Resulting information remains subject to the applicable purpose, recipient, retention and further-use restrictions.

(ii) **No Sale or Exchange of Information Access.** SHN shall not sell Participant information, Individual Data, Message content, Audit Log information or other operational information obtained or generated through Network functions or SHN services, including information derived from them, or accept access to that information as consideration. No service arrangement, Service Order, Member Terms or Data Processing Agreement may authorize such a sale. SHN may charge for a separately authorized service or result within its permitted inputs, purposes, actions, outputs, recipients and retention. Describing an information sale as a service does not make it permissible.

(iii) **Authority for Additional Uses.** Before using information for an Additional Service or additional result, SHN shall establish and document authority for the specified inputs, processing, outputs and recipients. The authorizing person must hold the relevant rights or act under a valid mandate from the person holding them and may authorize only processing within that authority. Authorization remains subject to applicable law, Individual rights, confidentiality obligations, source and recipient restrictions, and applicable processing agreements, including confidentiality duties under the applicable Network Participation

Agreement. Possession or lawful receipt of information does not itself establish authority for an additional analytical or commercial use.

(iv) **Reusable Scope.** An express authorization may cover a defined service or program and recurring outputs within identified scope and duration. Existing authority may be relied upon where documented and sufficient for the proposed use. Required consent from another person shall be obtained before the dependent processing. Approval of a service category or commercial terms does not supply missing authority. Results identifying and evaluating another Participant on a performance metric remain subject to the consent requirement in the definition of Network Intelligence. The separately authorized Network-utilization reports remain governed by Section 2.7(b) and its specified purposes and safeguards.

(v) **Hub Boundary.** The Hub remains subject to the Six Commitments and shall not access Message content.

(d) **Service-Use Records.** SHN shall maintain a current, versioned service-use record for each Network function and SHN service that processes Participant information or Individual Data, including the Hub, Network Trust Services, the registries under Section 2.6, Member Services and each Additional Service. Each record shall identify, as applicable, the purpose and principal; permitted inputs and sources; operator and suppliers; processing actions; outputs and recipients; processing locations; key custody; retention; correction; and exit arrangements. SHN shall make the records lawfully available to the Network Accountability Office for its assigned work and to the Data Rights Trust within its enumerated information and determination powers. An affected Participant may obtain a relevant summary on reasonable request. One maintained record may cover a reusable service configuration, with supplements identifying material differences in principal, authority, data or operation. A record documents established authority. Its availability to the Trust creates no general service-approval, audit or investigative responsibility.

2.8 **Authorized Third Party Services**. SHN shall maintain a process for qualifying Authorized Third Party Service Providers against published, objective requirements appropriate to the services and Network functions they perform. Qualification shall identify the approved functions, scope, and applicable conditions. Qualification does not itself appoint a provider to act for a Participant or Member or authorize access to their information.

(a) **Agreement with SHN**. Each Authorized Third Party Service Provider shall enter into an agreement with SHN establishing its permitted Network access and functions, applicable qualification requirements, operating and security responsibilities, information-use restrictions, incident and cooperation duties, and allocation of liability. The agreement shall incorporate these Network Rules by reference and may address those matters through an applicable Network Participation Agreement or other provider agreement. Any fees charged by SHN under the provider agreement shall relate to separately purchased services or separately licensed proprietary intellectual property and shall not impose a charge for included Network functions or required qualification. Rights granted under an applicable open-source license shall remain governed by that license.

(b) **Customer Agreement and Appointment**. Before providing an Authorized Third Party Service to a Participant or Member, the provider shall establish an agreement identifying the services, responsibilities, fees, information handling, and applicable termination and transition arrangements, and incorporating the applicable requirements of these Network Rules. An existing agreement, amendment, incorporated schedule, or authorized multi-party or sponsored arrangement may satisfy this requirement; an otherwise sufficient agreement need not be replaced solely because it predates Network participation. Each principal's required assent and any appointment or authority to act on its behalf or access information shall be established for the relevant scope. SHN may review provisions and evidence reasonably necessary to establish Network compliance, subject to privilege and protection of unrelated confidential terms.

(c) **Consistency with Network Rules.** An Authorized Third Party Service Provider shall not use its customer or provider agreements to waive applicable Network protections, expand information-use rights beyond the authority granted, or restrict a Participant's or Member's independent Network rights. As between SHN and the provider, these Network Rules shall control over inconsistent provider-agreement terms concerning Network participation or use. The provider shall correct any inconsistent customer-agreement provision to preserve the applicable Network requirements. A provider may charge for its own services. It shall not describe those charges as Network access, participation, or transaction fees, or represent that purchasing its product or service is required to obtain Network participation, Open Access functions, or Individual rights that are available without it.

2.9 Information Blocking Compliance. SHN and each Participant shall comply with 45 CFR Part 171, to the extent applicable to that entity, in connection with its Network activities and the Network requirements for which it is responsible. Each remains responsible for its own compliance. SHN shall assess Network requirements and practices affecting access, exchange or use of electronic health information, including fees and third-party cost pass-throughs, qualification, suspension, non-activation and transition requirements, for consistency with those obligations. When relying on an exception, the responsible entity shall satisfy its applicable conditions and document the basis for that reliance. Failure to meet an exception does not by itself establish information blocking. This Section does not authorize a disclosure otherwise prohibited by law or expand any person's authority to access information.

3. GOVERNANCE OF THE NETWORK.

3.1 Governing Bodies.

(a) **SHN.** SHN is responsible for the Network functions and infrastructure it undertakes to provide or operate, subject to these Network Rules and the powers reserved under the Governing Instruments. The SHN Board governs the business and affairs of SHN, and SHN management is responsible for day-to-day operations.

(b) **Governance Council.**

(i) **Responsibilities.** The Governance Council protects the Network's neutrality and public-purpose governance. Participating public jurisdictions elect its Trustees through the geographically based election arrangements established in its Governing Instruments. The Council exercises two principal responsibilities:

(1) **Board elections and governance protection.** The Council exercises the director-election and reserved-approval rights attached to the Governance Council Share, including the transition to election of the entire SHN Board under the Governing Instruments. Specified changes affecting corporate control or the Council's governance rights and protections require Council supermajority approval under those instruments.

(2) **Approval of protected Network changes.** The Council approves material amendments to these Network Rules and the standard Network Participation Agreement, changes to protected participation rights, mandatory financial obligations and included functions, and other matters reserved to it under the Governing Instruments. SHN shall obtain all required approvals before implementing a reserved change.

(ii) **Operations.** The Governance Council Governing Instruments establish jurisdiction eligibility and participation, geographic representation, Trustee qualifications, selection and election procedures, terms, decision-making processes, conflicts requirements, and permitted compensation and expense reimbursement.

(iii) **Limitation on Authority.** The Governance Council acts only within the authority assigned to it under the Governing Instruments. It does not direct SHN's day-to-day operations, products, personnel, or routine commercial decisions. Trustees act in furtherance of the Council's purpose and are not instructed representatives of the jurisdictions that elect them. SHN directors elected by the Council exercise their own duties to SHN and are not subject to Council instructions.

(c) **Data Rights Trust.**

(i) **Responsibilities.** The Data Rights Trust independently protects the patient-data rights of Individuals as a class, whether or not they become Members. Its purpose is to preserve the rights established in its Governing Instruments and the Patient Rights Floor in Section 3.4(b) as the Network develops.

Through the Data Rights Trust Governance Share and its other assigned powers, the Trust reviews proposed changes affecting those rights, grants or withholds approval where its consent is required, and makes patient-rights determinations and certified findings on matters within its jurisdiction. Its information, Board observer and escalation rights support these responsibilities, subject to the protections established in the Governing Instruments.

The Trust makes its determinations on the factual record developed by the Network Accountability Office and other lawfully submitted materials. The Office conducts investigations and manages follow-up; SHN and responsible operators carry out operational remediation. The Trust's powers are those expressly assigned by its Governing Instruments.

(ii) **Internal Governance.** The Trust's Governing Instruments establish independent trustee selection and self-perpetuating succession, regional activation, qualifications, terms, conflicts requirements and internal procedures. They preserve independence from SHN, the Governance Council, participating public jurisdictions and Participants. The Trust's own administration, financial accountability, governance reviews and independent legal representation remain governed by those instruments.

(iii) **Record-Based Determinations.** The Trust decides matters within its enumerated jurisdiction on the record supplied by the Network Accountability Office, relevant Audit Log information and reports available under these Network Rules and the Governing Instruments, and other lawfully submitted materials. It may refer a specific record deficiency to the Office under Section 3.3(h). Independent legal and technical advisers may interpret that record and advise on the Trust's assigned rights within this record-based role. The Trust does not conduct or commission Network investigations, administer complaints, command incident response, select or manage investigators, implement remedies, or independently verify remediation.

(d) **Participant Advisory Council.**

(i) **Responsibilities.** The Participant Advisory Council provides structured advice concerning Network operation, implementation, and the development and amendment of these Network Rules and the Network Participation Agreement. It may propose amendments, submit recommendations, identify recurring issues, and establish working groups. SHN provides a disposition and rationale for substantive recommendations.

(ii) **Procedures.** The Participant Advisory Council operates under bylaws establishing its composition, qualifications, appointment process, terms, and procedures. Membership reflects relevant Participant, purchaser, operator, patient, community, and other stakeholder perspectives and is not limited to representatives of Participants with an effective Network Participation Agreement.

(iii) **Compensation and Expenses.** Any compensation or reimbursement of reasonable expenses for Participant Advisory Council service is governed by its bylaws and applicable SHN compensation policies.

(iv) **Limitation of Authority.** The Participant Advisory Council performs an advisory role only. It does not operate the Network, bind SHN, amend these Network Rules or the Network Participation Agreement, or exercise powers reserved to the SHN Board, Governance Council, or Data Rights Trust. Its consent or approval is not required for an amendment adopted in accordance with the applicable amendment process.

3.2 Amendments to the Network Rules or Network Participation Agreement.

(a) **Proposing Amendments**. SHN, the Governance Council, the Data Rights Trust, the Participant Advisory Council, any Participant, and any Individual may propose amendments to these Network Rules, including the Rule Documents, Open Access and Fee Structure, and Transaction Catalog, or to the Network Participation Agreement. Proposals shall be submitted to SHN for initial review.

(b) **SHN Review.** SHN shall evaluate a proposed amendment within thirty (30) days after receipt and provide the proposer with its initial disposition and rationale.

(i) **Non-Material Amendments.** SHN may adopt, modify, or decline a non-material amendment that does not affect a matter reserved for approval under these Network Rules or the Governing Instruments. SHN shall maintain a record of its classification and the basis for it. Classification shall be determined by the effect of the change, regardless of its document, technical form, commercial label or location. A change affecting a reserved matter remains subject to the required approval and assent wherever implemented. Changes to common liability, indemnification, dispute resolution, or financial obligations, and changes to an incorporated processing agreement that expand permitted Uses or Disclosures, reduce privacy, security, Individual-assistance, notification, retention, return or destruction protections, or alter liability or remedies, shall be treated as material. The Governance Council or Data Rights Trust may review a classification within its respective authority under the Governing Instruments.

(ii) **Material Amendments.** SHN shall submit a material amendment proposed by the Governance Council, Data Rights Trust, or Participant Advisory Council to the Governance Council and, where applicable, the Data Rights Trust for review and a decision on whether to approve the amendment. SHN may decline to advance a material amendment proposed by another person, but shall obtain all required approvals before adopting any material amendment. With any submission, SHN may provide commentary, an alternative proposal, or a recommendation for approval or rejection.

(c) **Governance Council Review and Approval.** The Governance Council shall review a submitted proposal and decide whether to approve it, decline it, or recommend modifications within three (3) months after receipt. Approval requires the affirmative vote of a majority of its voting Trustees, except that an amendment to the Six Commitments requires the affirmative vote of at least two-thirds of its voting Trustees, in each case subject to the applicable quorum, voting, and other requirements of the Governing Instruments. Any revised proposal shall receive the approvals required for its final text before adoption by SHN. Failure to act within the review period does not constitute approval.

(d) **Data Rights Trust Review and Approval.** SHN shall submit substantive changes to any Six Commitment to the Trust for record-based review within its enumerated jurisdiction. Trust approval is required for matters expressly reserved under its Governing Instruments, including changes materially impairing the enumerated patient-data rights. Changes to routine implementation, service-use records or product launches require no Trust approval solely because they concern information. The governance-reference record in Section 3.4(a) identifies the applicable source authority. Neither body may waive the Patient Rights Floor. Where both approvals are required, each shall separately approve the same final text; without a required approval the change does not take effect.

(e) **Publication and Effectiveness**. SHN shall publish adopted amendments, making them available to all Participants and Individuals, and shall deliver direct notice of them to each Participant on the date of publication, so that the notice periods under each Network Participation Agreement run from the same date. Publication and direct notice shall occur at least thirty (30) days before the effective date and include a concise explanation of the changes

and identification of the approvals obtained, where required. An amendment to the Network Participation Agreement applies to an existing Participant only in accordance with the amendment provisions of that Participant's agreement. Publication does not substitute for required approval or assent. Operational and security updates remain subject to their applicable notice and implementation requirements; they may not change protected rights or obligations without the approvals required by this Section.

(f) **Ordinary Expansion and Operational Changes.** Within the authorized framework, SHN management under Board oversight may add Transaction Types, expand geographic availability, introduce, expand and price optional services within authorized categories, and implement established technical and qualification requirements. New capabilities receive the explicit fee designation required by Section 2 of Exhibit A. Existing contractual commitments, included functions and Individual rights remain protected. These ordinary decisions require no separate Council or Trust approval unless their effect reaches a reserved matter. A new paid category requires the approval specified in Exhibit A. Material qualification-framework changes affecting protected participation rights follow the applicable approval process; routine test cases, configuration and qualification decisions within that framework remain operational functions. Removal of a Transaction Type requires Council approval and any applicable Trust approval. Retirement of an obsolete Specification version under Section 6.6 does not authorize withdrawal of protected scope. This allocation operates within the Certificate and the governing-body instruments identified under Section 3.4(a). SHN may issue, version and modify Transaction Specifications under Section 6.3 without separate Governance Council or Data Rights Trust approval, except where a change requires approval under these Network Rules or the Governing Instruments. A Transaction Specification may not amend protected participation rights, Open Access fee protections, the Six Commitments, Individual Rights or the allocation of liability under a Network Participation Agreement, or create a payment obligation. Applicable notice, qualification and transition requirements continue to apply.

(g) **Both-Shares Matters.** If the holders of the Governance Council Share and Data Rights Trust Governance Share disagree on a matter requiring both approvals that concerns protection or integrity of patient data or patient rights, the patient-protective status quo specified in the Governing Instruments shall be maintained. The holders shall identify their grounds and promptly use an expedited consultation or facilitated resolution process permitted by those instruments. The Office may supply a focused supplemental factual record within its mandate. A facilitator may assist development of a revised proposal; the required consents remain with their authorized holders. SHN shall communicate the next resolution step and applicable interim protection to affected parties to the extent lawful. Delay supplies no deemed consent. Mandatory law, the Patient Rights Floor and access to the competent court remain controlling.

(h) **Initial Adoption and Effectiveness.** The initial adoption notice shall identify the exact texts and versions approved, the Governance Council's approval and date, and each approval or confirmation required under the Governing Instruments, including the Trust's confirmation that Section 3.4(b) reflects the Patient Rights Floor in its controlling instruments. It

shall state the effective date. The charter and trust provisions on which these Network Rules depend shall be operative by that date. Publication of a version label does not itself establish approval or effectiveness.

3.3 Complaints and the Network Accountability Office.

(a) **Scope.** SHN shall operate the Network Accountability Office to receive and address complaints from Individuals, their lawfully authorized representatives and Participants concerning Network participation, Network Transactions and services under these Network Rules. Former Participants and their authorized representatives may use the Office for matters concerning their prior participation, termination, evidence access and surviving rights. The remit includes relevant conduct of SHN, Participants and persons or services acting on their behalf.

(b) **Access.** The Network Accountability Office shall make available a clear description of who may file a complaint, how to submit one, and the process and expected timeframes for acknowledgment, review, investigation, and response. The process shall include a means of identifying urgent concerns involving ongoing unauthorized access, disclosure, or other material harm.

(c) **Independence, Conflicts and Confidentiality.** SHN shall provide the Office with resources reasonably sufficient for its responsibilities and maintain a documented conflict-handling procedure. SHN appoints and manages the Office and its day-to-day operations, subject to the independence and anti-retaliation protections in the Governing Instruments and the independent appointment and resourcing requirements in Section 3.3(d). Any Trust concurrence concerning removal of the head of the Network Accountability Office is confined to the independence and anti-retaliation questions expressly assigned by those instruments; it does not extend to routine hiring, investigative methods or operational priorities. Persons whose conduct is under review shall not control the investigation or disposition. Office personnel shall exercise independent judgment. Access to complaint information shall be limited to persons who need it for authorized investigation, advice, response, correction, oversight or legal duties, under applicable confidentiality and access controls.

(d) **Review and Investigation.** The Office shall promptly acknowledge and assess each complaint and investigate within its scope as reasonably necessary to establish the relevant facts. It controls investigative methods, personnel and evidence collection within its mandate and may arrange appropriate independent investigative assistance subject to lawful access and confidentiality.

Where a matter concerns senior SHN management, Office leadership, or another person who could materially control the investigation, its resources or the engagement of investigative assistance, the disinterested members of SHN's Board, acting directly or through a committee of disinterested directors, shall determine the need for independent handling and appoint and resource an independent investigator when required. The conflict-handling procedure shall designate in advance an independent appointing authority for matters in which no disinterested Board decision maker can lawfully act, consistently with applicable law and the Governing Instruments. A person whose conduct is under review shall not control the investigator's

appointment, scope, authorized evidence access or findings. The Trust may receive the completed record within its enumerated jurisdiction and may identify a specific deficiency under Section 3.3(h), but it does not select or direct the investigator.

The Office shall promptly refer urgent risks to the responsible operating functions; incident containment, reporting and restoration shall proceed without awaiting an Office or Trust determination. For matters outside its remit, the Office shall explain the disposition and identify an appropriate alternative channel where reasonably available.

(e) **Findings and Recommendations.** The Office shall report its factual findings and may recommend corrective action, including correction of information, remediation of controls or practices, and proportionate access or participation restrictions under these Network Rules. It shall refer an enumerated patient-rights matter requiring Trust determination with the relevant lawful record. Office findings and recommendations become certified Trust findings only through the ratification required by the Trust instruments. Other reserved matters shall be referred to the body with the relevant authority.

(f) **Response and Follow-Through.** SHN shall consider the Office's findings and recommendations in good faith and provide a documented response identifying adopted action or reasons for declining a recommendation. SHN and responsible operators perform the required correction, identify accountable owners and expected completion periods, and provide status and completion evidence to the Office. The Office tracks follow-up and may arrange appropriate verification within its mandate. It shall provide relevant status and completion records to the Trust for a matter before the Trust and may escalate unresolved matters through the existing Board, governance and contractual remedy routes. The Trust determines the effect of the supplied evidence within its jurisdiction. This process preserves all binding protective, notice, correction and continuity duties.

(g) **Notice to the Complainant.** The Network Accountability Office shall provide the complainant with a summary of its disposition, relevant findings, and any corrective action adopted or recommended, subject to applicable law and the protection of other persons' information, confidential information, and security credentials. If a complaint is not substantiated, the Office shall explain that conclusion. Where review remains ongoing beyond the expected timeframe, the Office shall provide an appropriate status update.

(h) **Record Supplementation.** Where a record is insufficient to decide a matter within the Trust's jurisdiction, the Trust may identify the specific deficiency and refer it to the Office. The Office shall assess the referral, obtain lawful supplemental material within its mandate, and report its response and any remaining limitation. Any unresolved failure to provide an adequate record follows existing independence and escalation procedures. A referral does not supply any consent required to obtain supplemental material.

(i) **Certified Findings and Protective Measures.** A certified Trust finding shall identify the enumerated right, relevant record, ratified determination and rights-compliant result required within the Trust's existing authority. SHN shall promptly provide its written response and implement the required result through lawful measures selected by management and responsible operators. The response shall identify owners, milestones and any issue

requiring clarification. The Office shall track implementation and supply status and completion evidence. A request for clarification shall not delay independently required protective action. Any temporary Trust hold shall be confined to an affected proposed action, satisfy the material-and-irreparable-impairment standard in the Trust agreement, state its grounds and resolution deadline, and be implemented by SHN. Expiry of a temporary hold supplies no consent otherwise required for the action. These procedures confer no general damage-assessment, penalty-setting, operational suspension or incident-command power on the Trust.

(j) **Trust Interface.** The Data Rights Trust may exercise the consent, governance-share, certified-finding, publication and other rights expressly assigned to it under its Governing Instruments and these Network Rules. The allocation of responsibilities in Section 3.1(c) applies.

3.4 Constitutional Governance References and Patient Rights Floor

(a) **Governance-Reference Record.** SHN shall maintain an accurate, accessible record identifying the effective Certificate of Incorporation, bylaws, Council and Trust instruments, governance-share holding arrangements, current director-election stage, reserved approvals, voting thresholds for protected matters, applicable successor-preservation requirements, and the purpose-trust enforcer designation and contact where applicable. The record shall identify exact operative provisions and versions and be updated promptly following a material change. The record shall summarize the separate governance-share rights, applicable restrictions on investor returns and control, and the protections supporting governance independence. Where governance funding arrangements are relevant to those protections, SHN may satisfy this requirement by providing the relevant provisions or an accurate summary, subject to applicable confidentiality obligations. Corporate approvals, fiduciary duties, trust powers, funding obligations and remedies arise under their controlling instruments. The governance-reference record reports those protections and does not amend them or create additional bilateral rights. SHN shall make the operative Certificate of Incorporation, SHN bylaws, Council and Trust instruments, and Participant Advisory Council bylaws available to Participants and Individuals, subject only to redactions reasonably necessary to protect legally privileged or confidential information. Any redaction shall preserve visibility into the operative governance rights and protections.

(b) **Patient Rights Floor.** For the purposes assigned by the Data Rights Trust Governing Instruments, the Patient Rights Floor consists of the protected minimum stated below. The cited provisions identify where that minimum is implemented; citation of a provision does not make unrelated administrative, technical or commercial terms in the same provision part of the Floor. Entitled access and actions remain subject to lawful authority, appropriate identity verification and protection of other persons' information.

Protected minimum	**Implementing provisions**
Hub routing remains Message-blind and the Hub does not aggregate Message content or maintain a substantive Message repository	Sections 2.3(a)-(b)

Protected minimum	Implementing provisions
The Hub has no Message-decryption backdoor and key custody remains separated as required	Section 2.3(c)
Protected information is not sold, exchanged for consideration, or used for unauthorized secondary exploitation; authorized paid services remain limited to their established authority	Sections 2.7(c)(i)-(ii) and 5.8
Individuals have a usable route to entitled Network-activity information and core rights without compulsory membership, application download or service purchase	Sections 2.3(f), 5.1(a), 5.4(b), and 7.8(e)-(f)
Actions requiring Individual authority or consent use appropriately scoped authority, including representative authority where applicable	Sections 2.3(d), 5.5(a)-(c), and 5.6
Withdrawal, expiry or modification of an applicable consent or instruction governs dependent future actions as required	Section 5.5(c)
Network activity remains attributable and entitled persons have usable audit visibility, challenge and correction routes	Sections 2.3(e)-(f), 5.2(a)-(b), 5.7, and 7.8(a), (e)-(f)

4. PARTICIPATION IN THE NETWORK.

4.1 **Eligibility to Participate**. A natural person or legal entity may become a Participant if it falls within one or more of the following categories and satisfies the applicable participation requirements under these Network Rules:

(a) A Health Care Provider.

(b) A Health Plan.

(c) A Public Health Authority.

(d) An employer, healthcare purchaser, public program, technology or service provider, operator, or other person or entity with a lawful role in providing, purchasing, administering, supporting, or receiving healthcare or related services.

4.2 **Role of Authorized Actors**. A Participant may designate an Authorized Actor to act on its behalf within an identified scope of authority. The Authorized Actor's activities shall remain within that authority and the Participant's accepted and activated scope, where applicable, and shall comply with applicable Privacy Law and the Network requirements applicable to the functions performed. Any required designation, qualification, and access controls shall be established before the Authorized Actor performs the relevant activity. An Authorized Actor need not become a Participant solely to act on behalf of a Participant, but may become a Participant in its own capacity if it satisfies Section 4.1 and enters into a Network

Participation Agreement with SHN. An Authorized Actor's separate participation does not itself establish authority to act for another Participant.

4.3 Participant Onboarding Process.

(a) **Application and Participation.**

(i) **Application.** An Applicant shall submit an application in the form prescribed by SHN, containing information reasonably necessary to establish its identity, eligibility, and proposed participation. Required information may include legal name, address, applicable organizational identifiers, designated contacts, relevant lines of business, and the identity and authority of the person signing for the Applicant. Information concerning Authorized Actors, operators, capabilities, endpoints, proposed Transaction Types and roles, Qualified Transaction Paths, and deployment arrangements shall be provided to the extent relevant to the Applicant's proposed scope. Information needed solely for activation of a particular interaction may be supplied when that activation is requested. SHN may prepare application and Participant Profile information from information already supplied by the Applicant, subject to the Applicant's confirmation, and may incorporate sufficient current supporting records by reference.

(ii) **Review.** SHN shall review the application against applicable published participation requirements, including verification of the Applicant's identity and eligibility under Section 4.1. SHN may rely on sufficient current evidence from qualified sources and shall identify material deficiencies or additional information reasonably required to complete its review.

(iii) **Accession.** SHN may collect the application information and agreement signatures through a combined onboarding process. The Applicant may sign the Network Participation Agreement with its application or during SHN's review. SHN shall countersign promptly after verifying the Applicant's identity, eligibility and signatory authority and approving the application. The Applicant becomes a Participant when that agreement takes effect. SHN shall establish the Participant Profile, provide it to the Participant for review, and publish the information designated for public availability in the Network Directory. The Participant Profile shall distinguish accepted participation scope from production-activated scope. Participation does not require deployment of a Participant Gateway, purchase of Additional Services, or immediate activation of Network Transactions.

(b) Qualification and Production Activation.

(i) **Requirements.** Before initiating production Network Transactions within a particular role and scope, a Participant shall accept the applicable Transaction Specification and satisfy the qualification and activation requirements for its selected implementation and Qualified Transaction Path. Those requirements shall address the applicable operating responsibilities, actor authority, information-handling arrangements, controls, evidence, and recovery capabilities.

(ii) **Testing and Evidence**. SHN shall make available the applicable qualification requirements, testing procedures, and required qualification support. Testing may include sandbox testing using synthetic data, conformance tests, and review of relevant operating and security evidence. SHN shall reuse sufficient current qualification evidence where applicable and limit additional testing to requirements not established by that evidence. Synthetic testing may occur before accession under applicable test terms. Qualification requirements shall be objective, proportionate to the relevant functions and risks, and applied consistently to SHN-operated and alternative implementations. Purchase of an SHN service shall not substitute for qualification or confer preferential qualification treatment.

(iii) **Activation Record.** Upon satisfaction of the applicable requirements, SHN shall record the qualified implementation and activated Transaction Types, Specification versions or accepted compatibility rules, roles, scope, and paths. SHN shall not unreasonably withhold or delay qualification or activation and shall identify the reasons for any refusal or outstanding condition. Qualification or activation for one scope does not establish qualification or activation for another.

(iv) **Participant Gateway Deployment.** Hub Transactions require qualified Participant Gateway functionality under the applicable Transaction Specification. A Participant may satisfy this requirement through its own deployment or a qualified shared or operator-managed deployment. Gateway deployment is not required merely to become a Participant. The Participant, its appointed operator, or SHN shall establish and configure any Gateway used in accordance with the selected operating arrangement. The responsible operator shall establish and manage the required keys and credentials within its assigned responsibilities. Testing shall address the functions and paths the Gateway is intended to support, including Hub interoperability where Hub Transactions are proposed. A shared or previously qualified deployment may be used where it satisfies the applicable requirements and preserves each Participant's identity, authority, and information boundaries.

(v) **Changes and Requalification.** A Participant shall notify SHN of material changes affecting its qualified implementation or activated scope. Such changes may include changes to its operator, infrastructure, authentication or encryption controls, major software version, Transaction Types or roles, or processing location. SHN may require additional qualification or periodic reassessment where reasonably necessary under published requirements to establish continued conformance. Reassessment shall address the affected scope and reuse sufficient current evidence concerning unchanged elements. SHN shall identify the required work and applicable completion period. Failure to maintain required qualification may result in restriction or suspension of the affected activity in accordance with Section 4.4; it does not automatically terminate Participant status or unrelated qualified activities.

(vi) **Qualified Third Parties**. SHN may obtain information from qualified third parties or delegate specified onboarding, verification, testing, or qualification functions to them, consistent with applicable law and agreements. SHN remains responsible for the functions it delegates and the verification it undertakes. Reliance on an independent source does not, by itself, make that source an SHN subcontractor. Third-party evidence shall retain its relevant source, scope, and currency. An introduction, roster entry, or relationship with a third

party does not itself establish the Applicant's assent to the Network Participation Agreement, appoint an operator or Authorized Actor, or authorize access to Individual Data.

4.4 Participant Monitoring and Enforcement.

(a) **Audit and Monitoring.** SHN shall monitor Participants' participation in the Network for compliance with these Network Rules and the Network Participation Agreement. SHN, or a qualified entity acting on its behalf, may conduct compliance audits, subject to the following:

(i) SHN shall provide at least thirty (30) days' prior written notice identifying the scope of the audit and the information reasonably required.

(ii) An audit shall be limited to records, systems, activities, and controls reasonably relevant to the Participant's obligations under these Network Rules or the Network Participation Agreement. SHN shall take reasonable measures to minimize disruption to the Participant's operations, protect confidential information, and avoid unnecessary access to Individual Data. Monitoring and audits shall remain consistent with the Six Commitments.

(iii) SHN shall consider sufficient, current audit reports, certifications, and other evidence already available and avoid unnecessary duplication.

(iv) SHN shall conduct no more than one routine audit in any twelve (12)-month period. Additional audits may be conducted where reasonably necessary to verify correction of an identified violation or address a reasonable belief of material noncompliance.

(b) **Investigation.** SHN may investigate a Participant where SHN has a reasonable basis to believe that the Participant has violated these Network Rules, the Network Participation Agreement, or applicable Privacy Law in connection with its Network participation. The notice and frequency limitations applicable to routine audits do not apply to such an investigation, an investigation of a Network Security Incident, or a narrowly tailored request for information based on a reasonable belief of noncompliance. The scope and manner of an investigation shall be reasonably proportionate to the matter under investigation. The Participant shall reasonably cooperate with the investigation, subject to applicable law and protections for privileged information.

(c) Suspension.

(i) **Grounds and Scope.** SHN may suspend a Participant's access to or use of the Network Infrastructure or its ability to engage in specified Network activities where SHN reasonably believes that the Participant has violated these Network Rules, the Network Participation Agreement, or applicable Privacy Law in connection with its Network participation, and suspension is reasonably necessary to address the violation or resulting risk. Suspension shall be proportionate and limited, where reasonably practicable, to the affected services, Authorized Actors, credentials, Transaction Types, roles, or Qualified Transaction Paths. SHN may suspend the Participant's participation as a whole only where a narrower restriction would not reasonably address the violation or risk. If the violation consists solely of nonpayment of fees, SHN may suspend only the services to which the unpaid fees relate.

(ii) **Notice and Opportunity to Respond.** Except for an emergency suspension, SHN shall provide at least fifteen (15) days' prior written notice stating the grounds, proposed scope, and effective date of suspension, together with the corrective actions or conditions required to avoid or lift it. The Participant may respond and provide evidence of correction during that period. SHN shall consider that response before imposing the suspension and shall not impose the suspension if the grounds have been adequately resolved.

(iii) **Emergency Suspension.** SHN may impose an emergency suspension without prior notice where, in its reasonable, good-faith judgment, suspension is necessary to prevent imminent harm to the Network Infrastructure, Individuals, or Participants, or to comply with applicable law. SHN shall provide notice promptly afterward, explaining the grounds, scope, and conditions for restoration to the extent permitted by law. SHN shall promptly review any response from the Participant concerning an emergency suspension.

(iv) **Correction and Restoration.** Where corrective action is required, the Participant may submit evidence of correction or a corrective action plan identifying the actions and proposed timeframe for resolving the grounds for suspension. SHN shall evaluate the submission promptly, and in any event within thirty (30) days, and shall accept it, identify reasonably necessary modifications, or explain its rejection. Approval of a corrective action plan does not by itself require restoration before necessary safeguards are in place. SHN shall promptly narrow or lift the suspension when the grounds for the affected restriction have been resolved, including through adequate interim safeguards. A corrective action plan is not required where SHN determines that the suspension was imposed in error.

(d) **Termination.**

(i) **Grounds.** SHN may terminate a Participant's Network Participation Agreement where SHN determines, in its reasonable, good-faith judgment, that:

(1) the Participant has committed a material violation of these Network Rules, the Network Participation Agreement, or applicable Privacy Law in connection with its Network participation that has caused, or presents a substantial risk of, significant harm to Individuals, other Participants, SHN, or the Network, and continued participation subject to narrower restrictions would not adequately address that harm or risk;

(2) the Participant has committed a material violation that cannot reasonably be remedied, or has failed to implement agreed corrective actions within the applicable timeframe after notice and a reasonable opportunity to do so;

(3) a suspension has remained in effect for at least three hundred sixty-five (365) consecutive days, the underlying grounds remain unresolved, and termination of participation as a whole is warranted in light of the scope and seriousness of those grounds; or

(4) the Participant no longer satisfies applicable participation eligibility requirements, or continued participation is prohibited by applicable law, and restricting the affected role, function or scope would not adequately address the grounds.

Exclusion from a particular government program does not require termination of unrelated lawful participation.

(ii) **Notice and Opportunity to Respond.** SHN shall provide at least fifteen (15) days' prior written notice of termination, identifying the grounds and effective date. The Participant may respond during that period, and SHN shall consider its response before making a final determination. SHN may maintain an appropriate suspension during that period. If applicable law requires termination sooner, SHN may shorten or omit prior notice and shall provide notice promptly afterward to the extent permitted by law.

(iii) **Effect.** Termination ends the Participant's status and authority to initiate new Network Transactions. SHN and the Participant shall perform any applicable transition, information-handling, record-retention, and surviving obligations under these Network Rules and the Network Participation Agreement, including the export and request rights of former Participants under Section 7.8(e). Nonpayment of fees for optional services, standing alone, shall not constitute grounds for termination of Network participation.

(iv) **Appeals.**

(1) A Participant may appeal a proposed or effective suspension or termination by providing SHN with a written explanation of its disagreement and supporting information. An appeal shall be submitted no later than six (6) months after the action takes effect. This deadline does not limit a Participant's ability to seek restoration from suspension based on correction of the underlying grounds.

(2) SHN shall arrange for review by a person or persons who were not responsible for the challenged decision. SHN shall provide a reasoned written decision within thirty (30) days after receiving the appeal. An appeal of an emergency suspension shall receive expedited review appropriate to the circumstances.

(3) The decision may affirm, modify, or reverse the action, or condition restoration on specified corrective measures. An appeal does not automatically stay the action, but SHN shall consider whether a stay or narrower restriction is appropriate while review is pending.

(4) This appeal process does not limit any applicable dispute-resolution rights under the Network Participation Agreement or the Participant's ability to submit a complaint to the Network Accountability Office.

4.5 **Voluntary Status**. Participation in the Network is voluntary. A Participant may terminate its participation for any or no reason in accordance with the terms of its Network Participation Agreement.

4.6 **Universal Participant Obligations**. Each Participant shall comply with the following obligations:

(a) **Participant Profile Updates.** Each Participant shall promptly notify SHN of changes to the information in its Participant Profile, including identifying information, designated contacts, Authorized Actors, endpoints, and Qualified Transaction Paths. SHN shall

promptly update the Participant Profile following reasonable verification. A Profile update does not itself satisfy any separate approval, qualification, or activation requirement under these Network Rules.

(b) **Use of Participant Profile and Network Directory Information.** Each Participant shall use information provided by SHN concerning another Participant for purposes of establishing or managing Network participation, facilitating Network Transactions or other Transactions that rely on such information, or fulfilling obligations under these Network Rules. Such use shall comply with applicable access and information-use restrictions. Availability of Profile or Directory information does not itself authorize access to Individual Data.

(c) **Responses to Data Requests**. A Participant receiving a request for data as part of a Network Transaction shall respond in accordance with the applicable Transaction Specification. The Participant shall provide requested data to the extent required by that Specification, provided that: (i) the request falls within the Participant's accepted and activated Transaction Type, role, and scope; (ii) the Participant maintains the requested data or has undertaken, within the accepted interaction, to retrieve it from an authorized accessible source, and has authority to disclose it; (iii) the Data Requestor is authorized to receive it; and (iv) the disclosure complies with applicable Privacy Law and these Network Rules, including applicable consent requirements. A Participant may withhold data where it reasonably determines that disclosure would risk harm to an Individual and withholding is permitted by applicable law and the applicable Transaction Specification. Where requested data is not provided, the Participant shall provide the applicable denial, exception, or error response, including the reason to the extent permitted by law. Responses shall use the Qualified Transaction Path accepted for the applicable Network Transaction.

(d) **Authorized Purposes and Scope.** A Participant shall initiate or respond to a Network Transaction only within the Transaction Types, roles, and scope included in its Transaction Schedule and activated for its participation. Each Network Transaction shall identify the applicable Transaction Type and comply with the applicable Transaction Specification, including requirements concerning purpose, authority, and consent.

(e) **Fee Payment.** A Participant shall pay fees, if any, properly due under these Network Rules and its applicable agreements with SHN, including any Service Order.

(f) **Reporting.**

(i) **Security Incidents**. A Participant shall report to SHN any known or reasonably suspected Network Security Incident as soon as reasonably practicable, and no later than seventy-two (72) hours after discovery, or sooner where required by applicable law or an applicable agreement. The initial report shall include information then reasonably available concerning the nature, likely scope, and potential Network impact of the incident and any containment measures taken. The Participant shall provide material updates as additional information becomes available. Reporting shall not be delayed pending a determination of fault or whether the incident constitutes a reportable breach under applicable Privacy Law.

(g) **Suspected Violations.** A Participant shall promptly report to SHN any known or reasonably suspected material violation of these Network Rules by itself or another person, providing the information reasonably available to support the report.

(h) **Cooperation**. A Participant shall reasonably cooperate with SHN in operating and protecting the Network and administering these Network Rules. Such cooperation includes timely responses to reasonable inquiries, provision of information reasonably necessary to investigate and address Network Security Incidents or suspected noncompliance, and prompt notification of credible cybersecurity threats to the Network Infrastructure. Requests for cooperation shall be proportionate to the matter involved and subject to applicable law, confidentiality obligations, and protections for privileged information.

(i) **Compliance with Law.** A Participant shall comply with applicable law, including applicable Privacy Law, in connection with its participation in the Network and use of the Network Infrastructure. Each Participant is responsible for establishing its authority to access, use, or disclose Individual Data, including obtaining or verifying any required Individual authorization or consent. Participation in the Network does not itself establish that authority.

(j) **Insurance.** A Participant shall comply with the insurance requirements set forth in its Network Participation Agreement.

(k) **Minimum Security Posture.** A Participant shall maintain a written information security program with administrative, technical, and physical safeguards appropriate to its Network activities and the volume and sensitivity of the Individual Data it processes, consistent with applicable requirements under these Network Rules. A Participant shall designate the Authorized Users permitted to access each applicable SHN-provided interface or service on its behalf and shall ensure that their access is appropriately authorized, reviewed, and promptly revoked when no longer permitted. The Participant shall perform its assigned responsibilities for credential issuance, protection, and management under the applicable access arrangements.

4.7 **Additional Obligations for Participants Using a Participant Gateway**. A Participant that uses a Participant Gateway, whether operated by the Participant, SHN, or an Authorized Actor, shall comply with the following obligations to the extent applicable to its assigned responsibilities under the deployment arrangement:

(a) **Gateway Deployment and Operation.** The Participant shall comply with the requirements of these Network Rules concerning Participant Gateway deployment, configuration, qualification, maintenance, and updates. The applicable deployment arrangement shall identify the responsibilities of the Participant and its Gateway operator.

(b) **Authorized Users of the Participant Gateway.** The Participant shall ensure that its Authorized Users use the Participant Gateway in accordance with these Network Rules and applicable Privacy Law. When engaging in Network Transactions, such Authorized Users shall act only within the Participant's accepted and activated Transaction Types, roles, and scope. The Participant shall reasonably monitor use within its control, promptly address unauthorized access or use, and report violations in accordance with the reporting requirements of these Network Rules. The Participant shall reasonably cooperate with SHN inquiries

concerning such use and promptly implement requests to restrict, suspend, or terminate an Authorized User's access made in accordance with the enforcement provisions of these Network Rules.

(c) **Connectivity Notification.** The Participant shall notify SHN as soon as reasonably practicable after becoming aware of a material connectivity failure or other operational issue affecting its Gateway's ability to support Network Transactions or potentially affecting the Network Infrastructure. The Participant shall reasonably cooperate with SHN and the applicable operator in diagnosing and resolving the issue.

(d) **Gateway Vulnerability Assessment.** The Participant shall conduct, or ensure that its operator conducts, a vulnerability assessment at least annually of the Participant Gateway deployment and connected systems within its or its operator's control that could materially affect Gateway or Network security. Where SHN operates the Participant Gateway, SHN shall perform the assessment for the components it operates, and the Participant remains responsible for its own connected systems. Sufficient, current assessments may be used to satisfy this requirement without duplicative testing. Each party shall promptly remediate critical or high-severity vulnerabilities within its assigned responsibilities that could affect Network security, applying interim mitigation where remediation is not immediately practicable.

4.8 **Additional Obligations for Certain Participants**. To the extent a Participant's processing of Individual Data in connection with the Network is not subject to comparable privacy obligations under applicable Privacy Law, the Participant shall:

(a) **Privacy Notice.** Maintain a prominent, publicly accessible, and understandable privacy notice describing its collection, retention, use, and disclosure of Individual Data in connection with the Network; applicable Individual rights and how to exercise them; and how to contact the Participant with questions or complaints. The Participant shall provide reasonable advance notice of material changes to those practices, except where an earlier change is required by law. A change to the notice does not itself authorize a new use or disclosure of Individual Data.

(b) **Safeguards.** Protect Individual Data in accordance with the security requirements of these Network Rules, including appropriate safeguards against unauthorized access, use, disclosure, alteration, or loss.

(c) **Individual Access.** Provide a reasonable means for Individuals to request and obtain access to Individual Data maintained about them in connection with the Network, subject to appropriate identity verification, applicable law, and protection of other persons' information. Where the Participant maintains such data solely on behalf of another party, it shall assist that party in responding to the request or direct the Individual to the appropriate party. Any denial or limitation shall be explained to the Individual to the extent permitted by law.

(d) **Accountability and Training.** Designate an officer or other senior official responsible for compliance with these privacy obligations and provide appropriate training to personnel who handle Individual Data or perform relevant Network functions.

(e) **Complaints.** Establish and clearly communicate an accessible process for receiving and responding to Individual complaints concerning the Participant's handling of Individual Data in connection with the Network.

(f) **Vendors and Contractors.** Require vendors and contractors processing Individual Data on its behalf to comply with applicable protections consistent with this Section through binding written obligations. Such obligations shall limit processing to authorized purposes and require appropriate safeguards and cooperation with Individual requests and complaints.

5. INDIVIDUAL RIGHTS AND MEMBER SERVICES.

5.1 Individual Rights and Member Relationship.

(a) Each Individual shall have the rights established by these Network Rules concerning Network activity and Individual Data relating to that Individual, whether or not the Individual is a Member. SHN shall provide usable means of exercising those rights, subject to appropriate identity and representative verification and applicable law. Exercising those rights shall not require establishing a Member relationship, downloading an application, purchasing a service, or paying an SHN fee. Independently provided applications may charge for their own additional services, but a usable route to required rights shall remain available without purchasing them.

(b) An Individual may establish a direct relationship with SHN under the Member Terms to receive Member Services. That relationship may be established through an SHN interface or a supported interface provided by a Participant or qualified third party. An invitation from a Participant, the exchange of Individual Data, or use of an independently provided application does not, by itself, establish a Member relationship. A Member's accepted roles and scope for supported Network Transactions shall be established through the Member Terms and applicable service terms, subject to the applicable Transaction Specification. A Member need not enter into a Network Participation Agreement or maintain a Participant Transaction Schedule unless separately participating as a Participant.

(c) A Member's relationship with SHN may continue across changes in providers, Health Plans, applications, or other introducing institutions. Providing or embedding a Member Service does not transfer or displace a Participant's relationship with the Individual.

5.2 Visibility into Network Activity.

(a) Each Individual shall have the right to access Metadata maintained by the Hub concerning that Individual. SHN shall make that information available in an understandable form identifying, to the extent recorded and applicable, the participating institutions, the nature of the interaction, relevant dates and times, and the transport events observed by the Hub. Access shall protect other persons' information and security credentials; any withholding or redaction shall be limited to what is necessary under applicable law or to protect such information or credentials.

(b) Each applicable Transaction Specification shall identify the evidence of Network activity to be made available to entitled Individuals, the party responsible for providing it, and the means of access. For a Qualified Transaction Path other than the Hub, qualification shall establish how the path supplies the required evidence and Individual access without requiring the underlying Message to pass through the Hub.

(c) Member Services may present entitled Metadata together with authorized information from Participants and other qualified sources, including source status, decisions, requests for information, and available next actions. Such presentation shall preserve the distinction between an observed transport event, a source statement or decision, and a service's interpretation. Receipt of a Message shall not be presented as application acceptance, approval, payment, or completed care without supporting evidence. A displayed status, notification, acknowledgment, or transport event does not by itself constitute formal notice, filing, or service, or commence or satisfy a legal or contractual period. Such effect applies only as established by applicable law or an expressly accepted arrangement identifying the responsible party, required content, delivery evidence, and timing basis.

(d) Information presented shall identify its source and relevant time and distinguish known status from missing, uncertain, disputed, or stale information. Nothing in this Section authorizes the Hub to access Message content or permits disclosure beyond the recipient's entitlement.

5.3 **Member Services.**

(a) Member Services enable Members to understand and act on healthcare-related activity across participating institutions. Supported functions may include:

(i) viewing relevant Network activity and authorized source information;

(ii) receiving status updates and notifications;

(iii) identifying the responsible institution and available next actions;

(iv) making requests, responding to requests, and exercising supported choices;

(v) authorizing representatives and managing their access; and

(vi) raising questions, challenging inaccurate information, and following the resolution of a correction request.

(b) SHN shall describe each Member Service's supported functions, source coverage, material limitations, and available channels in the applicable Member Terms or service specification. Once SHN undertakes a Member Service, it shall provide that service in accordance with those commitments and these Network Rules. A Member Service shall not be represented as providing complete visibility into activity for which it lacks an authorized, reliable source.

(c) SHN shall preserve continuity of the Member relationship and access to entitled information when a Member changes supported applications or introducing institutions, subject to applicable authority and retention requirements. Ending an optional institutional

service shall not, by itself, terminate the Member relationship or extinguish applicable Individual rights.

5.4 **Delivery Through Participant and Third-Party Applications.**

(a) Member Services and other capabilities supporting Individual rights may be made available through SHN interfaces, Participants' own applications, and qualified third-party applications and services. Members may use supported channels of their choice, subject to applicable qualification, authentication, and information-access requirements.

(b) SHN shall make available to qualified applications the interfaces and entitled information reasonably necessary to perform their supported functions under published, objective requirements.

(c) Where an application embeds an SHN Member Service, SHN remains responsible for the Member Service functions it undertakes, and the application provider remains responsible for its assigned functions. Where a provider supplies an independent service using Network capabilities, that provider shall establish its own service relationship and responsibilities under the applicable requirements for Authorized Third Party Services. Such use does not itself establish a Member relationship with SHN.

(d) Each application's access shall be limited to the information and actions authorized for its functions. Providing an interface, introducing a Member, or displaying one interaction does not confer access to the Member's other Network activity or authorize unrelated use of Individual Data.

5.5 **Individual Choices, Consent, and Instructions.**

(a) Where Individual consent or another Individual instruction is required by applicable law or the accepted Transaction Specification, the responsible parties shall obtain or verify that consent or instruction before performing the dependent action. Its scope shall identify, as applicable, the information, purpose, action, recipient, representative, Transaction Type, and effective period. Consent to one use shall not be treated as consent to another.

(b) SHN shall provide supported means for Individuals to record, review, and withdraw applicable consents and instructions. A Qualified Transaction Path shall not be activated for an interaction requiring such consent or instruction unless the responsible parties can obtain and enforce its current status. These functions may be performed through the Member Gateway or another qualified mechanism.

(c) Withdrawal, expiry, or modification shall be applied to dependent future actions in accordance with applicable law and the governing terms. SHN and the responsible parties shall maintain attributable records of relevant choices and changes, including their scope and effective time. SHN shall also maintain attributable records of Individual access requests and their disposition, including requests made through supported third-party interfaces. Such records shall follow applicable information-use and retention requirements and shall not introduce substantive Message content into the Hub Audit Log.

(d) Member activation, communication preferences, and authority to access or disclose source information shall remain distinct. Permission to receive a notification does not itself authorize retrieval, analysis, or further use of the underlying information. An otherwise authorized institutional Network Transaction shall not generally depend on the Individual establishing a Member account.

5.6 **Representatives and Delegated Access.** An Individual's lawfully authorized representative may exercise rights, receive information, and take supported actions within the representative's established authority. SHN shall provide supported means to establish, verify, review, and, where applicable, modify or revoke representative access. Account possession alone does not establish representative authority. Access and actions shall remain attributable to the representative and limited to the applicable scope.

5.7 **Questions, Challenges, and Correction**. SHN shall provide a usable process for Individuals and their authorized representatives to question or challenge information concerning them, including an incorrect identity association, representative designation, or displayed status. SHN shall acknowledge the request, identify or refer it to the party responsible for the contested information, and communicate its disposition and appropriate status updates. Each responsible Participant shall reasonably cooperate in investigating and resolving the matter. Where a credible challenge indicates ongoing exposure of another person's information or use of disputed representative authority, the responsible service shall promptly apply proportionate interim safeguards while investigating, without treating the challenge alone as proof that the source record is incorrect. SHN and the responsible parties shall apply confirmed corrections to affected services and records within their control and propagate them as required by the applicable specification. Confirmed wrong-person information shall cease to appear in the incorrect Individual's view. Necessary historical evidence may be retained under applicable access and retention restrictions. This process does not replace applicable appeal rights or the complaint process established elsewhere in these Network Rules.

5.8 **Member Terms and Information Handling.** SHN shall comply with the Member Terms and shall clearly identify the functions it undertakes, supported channels, information uses, retention, and applicable exit arrangements. Information processed on behalf of a Participant shall retain its applicable protections when used in an authorized Member Service. A Member relationship or choice of application does not grant SHN, a Participant, or an application provider a general right to combine, analyze, disclose, or otherwise use Individual Data for unrelated purposes.

5.9 **No Member Fees**. SHN shall not charge Members any fees, including fees for Member Services.

6. AUTHORIZED INTERACTIONS AND TRANSACTION FRAMEWORK.

6.1 Authorized Network Activity.

(a) A Participant shall engage in Network Transactions only within its accepted and activated Transaction Types, roles, and scope and in accordance with the applicable Transaction Specification. Each party remains responsible for establishing the authority required for its actions, including applicable authority to act for another person or to access, use, or disclose Individual Data. Inclusion in the Transaction Catalog, acceptance in a Transaction Schedule, or production activation does not itself supply that authority. Sufficient existing lawful authority may be used for a Network Transaction without reconstructing the underlying relationship. A change of path or operator does not expand that authority.

(b) Information provided to SHN shall be provided for an authorized Network function or service and handled in accordance with these Network Rules and the applicable participation, service, and information-use terms. Authority to process information for one function or service does not itself authorize its use for another.

(c) Qualification of a connection or path does not bring every exchange carried over it within the Network Transaction framework. Participants may use the same connection for other lawful activity under applicable arrangements, subject to continuing restrictions on information obtained through Network services.

6.2 Transaction Catalog.

(a) SHN shall maintain the Transaction Catalog identifying supported Transaction Types, their purposes, and applicable scope and geographic availability. The Catalog and related service disclosures shall distinguish available production capabilities from planned or testing capabilities.

(b) Listing a Transaction Type in the Catalog does not require a Participant to support it or establish the Participant's acceptance, qualification, activation, or authority to engage in it.

(c) SHN may add Transaction Types or expand their availability in accordance with the amendment and governance provisions of these Network Rules.

6.3 Transaction Specifications.

(a) SHN shall maintain or recognize an applicable Transaction Specification for each supported Network interaction. The Specification shall identify, as applicable, its purpose, participating roles, supported actions, representations, authority and consent conditions, required controls, response meanings, evidence, correlation, failure and recovery behavior, and implementation requirements. Responsibilities shall be assigned to the parties and services performing the relevant functions.

(b) The transaction framework may support Network-standard Specifications, reusable templates with permitted parameters, and scoped Specifications proposed by Participants. Each shall satisfy the applicable common requirements under these Network Rules. SHN shall maintain published procedures for reviewing and recognizing proposed Specifications and shall identify the reasons for any refusal or outstanding condition.

(c) A Specification or supported capability may be publicly discoverable, restricted to an eligible group, or private to the relevant parties. Discovery restrictions do not reduce applicable Network requirements. Publication of a Participant-provided Specification or confidential capability information requires the applicable rights or permission.

(d) A Transaction Specification shall not alter the Six Commitments, impose new fees, expand information-use rights, establish or expand direct counterparty contractual reliance rights, liability, remedies, or indemnities, or otherwise override these Network Rules or applicable agreements. Technical acceptance of a Specification does not itself constitute assent to such contractual changes. A change requiring approval or assent under those instruments shall follow the applicable process.

6.4 Participant Acceptance and Transaction Schedule.

(a) Each Participant's Transaction Schedule shall record its accepted Transaction Types, roles, scope, and applicable Specification versions or accepted compatibility rules. Acceptance may cover an eligible class of counterparties and recurring exchanges without requiring a separate agreement for each Network Transaction.

(b) No Transaction Type, role, or material expansion of scope shall be added to a Participant's Transaction Schedule without its agreement. Acceptance shall remain distinguishable from production activation.

(c) A Participant may request a modification to its Transaction Schedule. SHN shall respond within thirty (30) days and shall record the requested modification unless it conflicts with these Network Rules, falls outside supported scope, lacks required authority, or is subject to an applicable restriction or suspension. SHN shall identify the reason for any refusal and any outstanding conditions. A restriction affecting one activity shall not, by itself, prevent acceptance of unrelated scope.

6.5 Qualification, Activation, and Identification of Network Transactions.

(a) Before performing production Network Transactions, the applicable implementation and Qualified Transaction Path shall satisfy the qualification and activation requirements for the accepted roles and scope. SHN shall maintain records identifying the activated scope, applicable Specification, path, and assigned operating responsibilities.

(b) Each Network Transaction shall be identifiable as an exchange conducted under an accepted Transaction Specification, with a record of the relevant parties, their roles, the applicable scope, and the Qualified Transaction Path used. Participants may agree in advance that recurring exchanges meeting specified conditions will be Network Transactions, without separately approving each exchange.

(c) A Qualified Transaction Path may use the Hub or another accepted means of execution. Each path shall satisfy the requirements assigned to it for the supported interaction, including applicable authority, security, evidence, Individual rights, and recovery requirements. Qualification shall address the functions actually performed without requiring replication of an unused component.

(d) Once an interaction is identified as a Network Transaction, rejection, execution failure, or breach does not remove it from the applicable Network requirements. Attempted or purported use of a Network function remains subject to applicable security, information-use, incident-reporting, evidence-preservation, and enforcement requirements even if it does not qualify as an accepted Network Transaction. This does not bring unrelated lawful activity over the same connection within the Network Transaction framework.

6.6 Changes, Withdrawal, and Continuing Work.

(a) SHN shall identify Specification versions, material changes, applicable compatibility rules, and transition requirements. Publication of a revised Specification does not, by itself, expand a Participant's accepted roles, scope, information-use permissions, or financial obligations. Required updates within accepted scope remain subject to the applicable notice, qualification, and amendment provisions.

(b) SHN shall promptly record a Participant's requested withdrawal from a Transaction Type or role and identify when initiation of new Network Transactions will cease. Withdrawal or retirement of a Specification shall preserve applicable obligations concerning outstanding requests and responses, required evidence, information handling, and orderly transition.

(c) Changes in an operator, implementation, or Qualified Transaction Path shall not, by themselves, alter the meaning of an outstanding request, create a new business request, or restart an applicable deadline. Each subsequent action shall remain subject to current authority and the applicable continuity arrangements. The outgoing and incoming operators shall cooperate within their respective responsibilities to preserve required records and references, communicate outstanding status and deadlines, and distinguish known outcomes from uncertain outcomes. The successor shall use its own authorized credentials and establish continuing authority before acting. Required continuity and record-preservation duties shall not be conditioned on purchasing an additional archival service. Each operating arrangement shall identify a practicable means for an authorized successor to obtain required records or usable references, source status, pending work, timing bases, and uncertain outcomes if the outgoing operator is unavailable. The mechanism shall preserve current authority and information rights without requiring transfer of general predecessor credentials or unrelated information; it need not require a common SHN content archive.

6.7 Relationship to Member Services and Additional Services.

(a) Presentation of entitled Metadata or authorized source information through a Member Service does not, by itself, establish a separate institutional Transaction Type. A request or action initiated through a Member Service shall satisfy the applicable Transaction Specification and activated scope where it constitutes a Network Transaction.

(b) An Additional Service may use or coordinate Network Transactions, but its purchase does not expand the parties' underlying authority or Network permissions. The additional work, responsibilities, and information handling shall be established in the applicable Service Order. Any required processing instruments shall be in place before the relevant processing begins.

6.8 Jurisdiction Schedules and Conflicting Law

(a) Jurisdiction Schedules. SHN may adopt and publish Jurisdiction Schedules establishing additional legal and contractual requirements for Network activity in specified jurisdictions. Each Schedule shall identify its scope and shall be adopted and amended under Section 3.2.

(b) Protected Requirements. A Jurisdiction Schedule may supplement these Network Rules but shall not waive or diminish the Six Commitments or the Patient Rights Floor. Mandatory law applies whether or not reflected in a Schedule. Where affected activity cannot comply with both mandatory law and those protections, it shall not begin or shall be restricted, suspended or discontinued to the extent necessary.

(c) Conflicts and Resolution. SHN shall promptly assess credible legal conflicts, document and explain any resulting restriction to affected Participants to the extent permitted by law, and seek any required governance approval for a proposed resolution. Restrictions shall be limited to affected activity and lifted when their basis is resolved. Applicable notice, security, evidence-preservation and continuity duties remain in effect. A restriction reasonably necessary and otherwise compliant with this Section does not itself constitute a breach, but does not excuse a prior breach or failure to perform continuing obligations.

(d) Government Programs. Requirements specific to Medicare Advantage, Medicaid or other government programs shall be addressed through the applicable Government Program Addendum to the Network Participation Agreement before the affected functions begin.

6.9 Automated Interpretation. A service using automated interpretation to perform an assigned Network function or produce information transmitted in a Network Transaction or supplied as Network evidence shall:

(a) Maintain required authorization controls independently of model output, without expanding delegated authority or recipient access.

(b) Distinguish its inferences, summaries and material changes from information attributable to the original source. A Participant remains responsible for substantive decisions it adopts and issues as its own.

(c) Follow the review, traceability and retention requirements established for that function in the applicable Transaction Specification or service terms.

7. NETWORK SECURITY.

7.1 Security Responsibilities and Baseline Safeguards.

(a) SHN shall establish, implement, maintain, monitor, and periodically update reasonable, industry-standard technical, physical, and administrative safeguards for SHN-Operated Infrastructure and information processed in performing its Network and service functions. These safeguards shall protect the confidentiality, integrity, and availability of such systems and information, including Identifiable Individual Data regardless of whether it is PHI.

(b) SHN shall maintain a written information security program aligned with the then-current NIST Cybersecurity Framework and appropriate to the risks of the functions it performs. SHN shall implement controls reasonably designed to satisfy applicable requirements of the HIPAA Security Rule and, where applicable to the relevant systems or information, NIST SP 800-171. SHN shall maintain and periodically test business-continuity and disaster-recovery plans for SHN-Operated Infrastructure and the lawful preservation and restoration of required records.

(c) Participants and their appointed operators remain responsible for security within their assigned operating scope. Each qualified implementation and operating arrangement shall identify responsibility for applicable security controls, credential and key management, monitoring, remediation, and incident response. SHN's recognition of a Qualified Transaction Path does not itself make SHN responsible for operating that path. SHN remains responsible for functions it undertakes, including functions it delegates to suppliers acting on its behalf.

7.2 Independent Assessments and Remediation.

(a) SHN shall obtain an independent third-party security assessment and technical audit of SHN-Operated Infrastructure at least annually. The assessment shall address the safeguards required by Section 7.1 and include penetration testing of internet-facing systems and vulnerability assessments of internal systems within SHN's operating scope.

(b) Assessors shall have qualifications and experience appropriate to the work performed and be independent of the functions being assessed, without conflicts that would impair their judgment.

(c) SHN shall evaluate identified findings, assign responsibility for remediation, and track corrective actions to completion within timeframes appropriate to their severity and risk. Where immediate remediation is not practicable, SHN shall implement appropriate interim safeguards.

(d) Upon a Participant's reasonable request, SHN shall provide a meaningful summary of assessment results relevant to the services provided to that Participant, including the status of material remediation, subject to confidentiality obligations under the Network Participation Agreement. SHN may withhold details that would expose security vulnerabilities, credentials, or another person's confidential information.

(e) A Participant shall not conduct penetration testing, vulnerability scanning, or other active security testing of SHN-Operated Infrastructure without SHN's prior written consent. Approved testing shall follow an agreed scope and procedures, and the Participant shall provide SHN with the results and identified vulnerabilities. This restriction does not prevent a Participant from reviewing supplied security evidence or assessing systems it operates, provided the assessment does not actively test SHN-Operated Infrastructure.

7.3 Encryption and Key Management.

(a) Messages transmitted through the Hub shall be encrypted by the applicable Gateway before transmission and remain encrypted while handled by the Hub. The Hub shall not possess or have direct or indirect access to Message-decryption keys or other capabilities enabling it to decrypt Messages.

(b) Each responsible operator shall generate, protect, manage, rotate, revoke, and recover keys and credentials within its assigned scope in accordance with applicable security requirements. Where SHN operates a Gateway or another service capable of processing readable information, SHN shall maintain separation of key custody, privileged access, and administration sufficient to preserve the Six Commitments.

(c) SHN shall maintain published cryptographic requirements appropriate to supported functions, specifying minimum algorithms, security strengths, key-exchange and authenticated-encryption requirements, protection of information in transit and at rest, and key lifecycle management for each supported function. Changes shall follow applicable notice and update procedures.

(d) A Qualified Transaction Path other than the Hub shall satisfy the confidentiality, integrity, and key-management requirements applicable to its accepted Transaction Specification and operating arrangement.

7.4 Security Leadership. SHN shall maintain a chief information security officer, or named delegate, responsible for SHN's information security program, oversight of security within SHN's operating scope, and coordination with Participants and other operators concerning Network security.

7.5 Insurance. SHN shall maintain the insurance policies required by the Network Participation Agreement.

7.6 Incident Reporting and Response.

(a) SHN shall notify each Participant likely affected by a known or reasonably suspected security incident involving unauthorized access, use, or disclosure of that Participant's information, or a material compromise of the confidentiality, integrity, or availability of SHN-Operated Infrastructure supporting that Participant. SHN shall also notify a Participant upon becoming aware of a Network Security Incident likely affecting that Participant. Notification shall not depend on a final determination of cause, fault, or whether the incident constitutes a legally reportable breach.

(b) SHN shall provide notice as soon as reasonably practicable and no later than seventy-two (72) hours after discovery, or sooner where required by applicable law or agreement. The initial notice shall contain information then reasonably available, including the nature and likely scope of the incident, affected systems or information, potential impact, containment measures, and any actions reasonably requested of the Participant. SHN shall not delay initial notice because its investigation is incomplete.

(c) SHN shall provide material updates as additional information becomes available and a summary of findings and corrective actions upon completion of its investigation, subject to applicable law and protection of other persons' information and sensitive security details.

(d) SHN shall promptly investigate, contain, mitigate, and remediate incidents within its operating responsibility. SHN, affected Participants, and responsible operators shall reasonably cooperate in responding to incidents affecting Network Transactions, including those using non-Hub Qualified Transaction Paths. Each party remains responsible for notices and other actions assigned to it under applicable law and agreements. Coordination shall not delay required protective action or notification.

(e) **Allocation of Costs and Liability.** Subject to the limitations in the Network Participation Agreement and applicable processing agreement, SHN shall be responsible for reasonable and documented costs incurred by a Participant in investigating, containing, and providing required notifications concerning a potential or confirmed Network Security Incident caused by the acts or omissions of SHN or its agents. Such costs include, as applicable: (i) a third-party assessment of whether Personal Data has been compromised; (ii) notices to affected Individuals, regulatory agencies, or the media required by applicable Privacy Law; and (iii) no-cost credit monitoring for affected Individuals to the extent and for the period required by applicable Privacy Law or a regulatory agency with jurisdiction. This provision does not expand liability beyond the limitations in the applicable agreements or permit duplicate recovery. A dispute concerning cost allocation shall not delay required notification, containment, mitigation, or cooperation.

7.7 Authentication and Access Controls.

(a) Each responsible operator shall implement authentication and access controls appropriate to its supported functions. Access shall be limited to authorized persons and services, reviewed periodically, and promptly modified or revoked when no longer authorized. Privileged and support access shall be restricted, attributable, and logged.

(b) Authorized Users accessing a Participant Gateway shall be authenticated through a methodology meeting the applicable requirements for Authenticator Assurance Level 2 under NIST SP 800-63. Automated services, applications, and agents shall use credentials and authentication mechanisms appropriate to their functions under applicable qualification requirements. Authentication does not itself establish authority to act for a Participant or Individual.

(c) SHN shall design and maintain authentication functionality for SHN-provided software within its supported scope and operate authentication and access controls for SHN-operated services. Participants and appointed operators using other qualified implementations shall maintain conforming controls within their assigned responsibilities.

7.8 Audit Logs and Transaction Evidence.

(a) **Hub Audit Log.** SHN shall maintain an attributable, tamper-evident Audit Log of every Hub Transaction, including rejection, failure, and recovery events observed by the Hub. The Audit Log shall contain the Metadata required by these Network Rules and applicable Transaction Specifications to identify and evidence those events. It shall not contain Messages or reproduce substantive Message content.

(b) **Integrity and Correction.** Audit Log entries shall be protected against unauthorized alteration or deletion. Corrections shall be recorded as linked subsequent entries preserving the original record during its applicable retention period. Retention and authorized deletion shall comply with these Network Rules and applicable law.

(c) **Retention.** Hub Audit Log entries shall be maintained for at least six (6) years from the date of the applicable Transaction, subject to applicable law. SHN shall maintain a versioned Retention Specification addressing recorded information, lawful retention, entitled access, correction, export and disposition, including applicable jurisdictional requirements. The Retention Specification is a Rule Document governed by Section 3.2, with Data Rights Trust review or approval required only to the extent provided in that Section and the Governing Instruments. A function whose required Hub record may contain PHI shall not be production-activated until lawful retention and access arrangements are established. The Retention Specification shall separately identify the permitted purposes, maximum retention periods and deletion triggers for temporary encrypted Message transport state, including any permitted recovery copies, consistently with the Six Commitments and applicable processing terms. The six-year Audit Log period does not apply to that transport state and does not authorize retention of Message content.

(d) **Evidence on Other Components and Paths.** Participants, SHN and other responsible operators shall maintain the evidence assigned to their functions under the applicable Transaction Specification and operating arrangement. Qualification of a non-Hub Qualified Transaction Path shall identify the required evidence, responsible custodian, integrity protections, lawful retention period, entitled access and arrangements for continued availability after the connection or operating service ends. These arrangements shall be established before production activation. The Hub's six-year retention period does not automatically apply to another path. Required Individual access and essential continuity evidence shall not depend on an additional archival purchase after the service ends.

(e) **Access.** Each Participant shall have access to Audit Log entries concerning Transactions to which it was a party. Within thirty (30) days after its Network Participation Agreement ends, SHN shall provide the former Participant, without charge, a usable export of those entries and other evidence SHN maintains under this Section concerning its Transactions. SHN shall also provide access on verified request, within a reasonable time and without charge, for as long as those records are retained under the Retention Specification and applicable law. Such access shall not require renewed participation, a production connection or purchase of Additional Services. Records needed for an authorized handoff or applicable legal deadline shall be provided when required, without waiting for the thirty-day export deadline. SHN may decline a manifestly repetitive or excessive request only on an objective, proportionate basis. A request is not repetitive or excessive because of an incomplete or unusable prior export, SHN's failure, a material correction or new relevant events. Any refusal shall state its basis, identify usable information already supplied, offer a reasonably available narrower means of access and identify the Network Accountability Office review route. A restriction shall not defeat a mandatory right or urgent continuity need.

Each Individual shall have access to entries concerning Individual Data about that Individual. Access under this Section shall be subject to appropriate identity and authority verification and applicable law, and shall protect other persons' information and security credentials while preserving entitled visibility.

(f) **Means of Access.** SHN shall provide usable means of obtaining entitled Hub Audit Log information through supported interfaces, including qualified applications. Access shall not require deployment of a Participant Gateway or purchase of Additional Services.

EXHIBIT A: OPEN ACCESS AND FEE STRUCTURE

1. **Common Participation and Open Access.**

(a) SHN shall not charge Participants fees for Network participation, connection to the Network Infrastructure or Network Trust Services, including required onboarding.

(b) "Open Access" means a Transaction Type or defined scope designated in the Transaction Catalog as available without SHN transaction fees, regardless of connection count or Transaction volume. Open Access includes the common functions required by these Network Rules to establish and complete the supported exchange, including required qualification, common controls, entitled evidence and access, and common correction and continuity functions. The protection applies through the Hub and other Qualified Transaction Paths.

2. **Transaction Catalog**

(a) Exhibit B sets forth the initial Transaction Catalog. SHN shall maintain and publish subsequent versions on its website, identifying each Transaction Type's scope, availability, Open Access or paid designation, and applicable pricing or service-term reference. An entry containing both included and paid functions shall distinguish them.

(b) SHN may add Transaction Types and capabilities, including paid offerings, subject to Section 3 of this Exhibit. Listing or standardizing a capability does not itself designate it as Open Access. A legal requirement applicable to a capability does not, by itself, designate that capability as Open Access; applicable legal restrictions on charging remain controlling. Catalog listing does not establish production activation or agreement to pay.

(c) Updates shall identify their version and effective date and follow applicable notice and approval requirements. SHN shall retain accessible prior versions and a record of material changes. Updates do not require re-execution of individual Network Participation Agreements.

3. **Additional Services and Paid Offerings**

(a) SHN may offer Enhanced Support, Gateway Management, Network Management, Network Intelligence and Network Orchestration under Service Orders specifying the purchased scope, responsibilities and fees. These offerings may include implementation and other expressly scoped assistance within the authorized categories.

(b) Under Board oversight, SHN may develop, expand, bundle and price services and paid Transaction Types within those categories without separate Governance Council or Data Rights Trust approval, except where a decision requires approval under the Governing Instruments. A purchased service may encompass multiple Transactions and be priced as a complete service, workflow or result.

(c) A new paid category outside the authorized categories requires Governance Council approval of the category and its boundary with included functions, together with any other required approval.

(d) Before incurring fees, a purchaser shall expressly accept the purchased scope, payment responsibility, fees or pricing method, and fee-change terms in a Service Order or other agreement. Catalog publication or a Transaction Schedule entry does not create a payment obligation. A sponsored purchase does not impose payment responsibility on a beneficiary without its acceptance. Sponsorship does not itself authorize the sponsor to act for the beneficiary, access the beneficiary's information or restrict the beneficiary's choice of qualified operator. Sponsored arrangements shall comply with applicable law, and SHN may decline or condition an arrangement it reasonably determines would not comply.

4. **Operating Resources and Third-Party Costs**

(a) Participants remain responsible for hosting, Gateway operation, custom integration and other resources outside the included service scope. They may self-operate, appoint a qualified operator or purchase SHN services. SHN shall not use resource requirements to make supported Open Access functions available only through a paid SHN service.

(b) Participants are responsible for applicable third-party licenses and services attributable to their implementation or use. They may obtain these directly or expressly agree to SHN's procurement and pass-through of attributable costs, disclosed in advance and without markup. This provision does not permit recovery of ordinary common operating costs.

(c) SHN may defer new capabilities pending necessary qualification, licenses, operating arrangements and funding. Restrictions on existing capabilities remain subject to the Network Rules and applicable agreements.

5. **Protection of Included Rights**

(a) Existing Open Access scope shall retain its fee protection unless changed through the applicable amendment process, Governance Council approval and any other required approval. SHN shall not circumvent that protection through renaming, bundling, technical changes, Catalog removal or individual agreements. Introducing a mandatory participation charge requires the same approvals.

(b) Optional services shall not be required for participation or completion of an otherwise supported Open Access exchange. Ending or declining a purchased service does not itself end participation or Open Access rights, although continued Transactions require a qualified operating arrangement. Optional service scope and pricing may vary by agreement.

6. **No Member Fees.**

SHN shall not charge Members any fees, including fees for Member Services. The third-party cost provisions of this Exhibit do not authorize charges to Members.

7. **Incorporation.**

This Exhibit forms part of the Network Rules. Capitalized terms not defined here have the meanings given in the Network Rules or Network Participation Agreement.

EXHIBIT B: INITIAL TRANSACTION CATALOG

1. Purpose and Maintenance.

This Catalog identifies Network Transaction Types, their scope, geographic coverage, and fee designation under Exhibit A. SHN shall maintain and publish subsequent versions on its website in accordance with the Network Rules.

The Geographic Scope column identifies the jurisdictions covered by each entry. SHN may add jurisdictions or designate an entry Global in accordance with the Network Rules. Applicable Transaction Specifications and the maintained Catalog shall identify jurisdiction-specific requirements and production availability. Geographic scope does not, by itself, establish authority for a cross-border disclosure or transfer.

Listing does not establish that every described capability is operational or that a Participant is qualified or activated to perform it.

2. Initial Transaction Types.

"Open Access" has the meaning and protections established in Exhibit A.

Transaction Type	Scope of Interaction	Geographic Scope	Fee Designation
Patient Access	An Individual or authorized representative requests and receives information from a provider, Health Plan, or other authorized source, directly or through an authorized application or service. Includes responses, delivery status, and supported updates.	United States	Open Access
Prior Authorization	Authorized parties discover applicable requirements; submit, supplement, or update requests; request additional information; and exchange acknowledgments, status, decisions, and corrections. Roles may include providers, Health Plans, designated	United States	Open Access

	review entities, and authorized supporting sources.		
Provider Access	An authorized provider requests and receives information made available by a Health Plan for the supported purpose, including applicable attribution, access-status, and response exchanges.	United States	Open Access
Payer-to-Payer	Health Plans request and exchange authorized information concerning an Individual, including acknowledgments, responses, and transfer status.	United States	Open Access
Directed Treatment Exchange	Authorized parties request, send, and receive information supporting treatment, including clinical records, summaries, and related acknowledgments or responses.	United States	Open Access
Public Health Reporting	Authorized parties submit reports and notifications to public health authorities and exchange related queries, acknowledgments, corrections, and responses.	United States	Open Access
Eligibility, Benefits, and Cost Information	Authorized parties inquire about and exchange available eligibility, coverage, benefit, cost-sharing, accumulator, and Individual-specific cost information. Includes reporting existing coverage and payer-responsibility information.	United States	Open Access
Enrollment and Coverage Maintenance	Authorized parties submit and respond to enrollment, disenrollment, and coverage-maintenance requests and	United States	Open Access

	exchange confirmations, status, and corrections.		
Claims and Encounter Transactions	Authorized parties submit claims and encounter information and exchange acknowledgments, acceptance or rejection, corrections, voids, and reversals.	United States	Open Access
Claims Status	Authorized parties request and receive claim status, including information about processing progress, outstanding requirements, and disposition.	United States	Open Access
Remittance and Payment-Information Exchange	Authorized parties exchange remittance advice, explanations of payment, adjustments, premium information, and payment instructions or status. This entry covers information exchange, not movement or settlement of funds.	United States	Open Access
Appeals and Reconsiderations	Authorized parties submit appeals or reconsideration requests and exchange supporting information, acknowledgments, requests for additional information, status, and decisions.	United States	Open Access
Referrals, Scheduling, and Care Transitions	Authorized parties send and respond to referrals, appointment requests, and care-transition communications, including acceptance, decline, confirmation, cancellation, and status.	United States	Open Access
Orders, Fulfillment, and Results	Authorized parties submit orders for healthcare items or services and exchange acceptance, clarification,	United States	Open Access

	fulfillment status, results, cancellations, and corrections.		
Prescribing and Medication-Benefit Exchange	Authorized parties exchange prescriptions, renewal and change requests, medication history, dispensing status, formulary information, and medication-benefit inquiries and responses.	United States	Open Access
Attribution, Quality, and Health Program Exchange	Authorized parties exchange rosters, attribution records, quality measures or reports, care-gap information, and health-program requests, responses, and status. This entry covers exchange of those records and results, and not any service to generate them.	United States	Open Access
Secure Interpersonal and Organizational Communication	Authorized persons and organizations exchange supported healthcare-related messages, including direct or group communications and related delivery acknowledgments.	United States	Open Access

3. Common Scope and Supporting Exchanges.

(a) Each Transaction Type includes the supporting documentation, attachments, acknowledgments, error responses, corrections, and status exchanges required by its applicable Transaction Specification. These are components of the supported interaction and do not require a separate Catalog entry merely because they use a separate message.

(b) Participants may act through Authorized Actors and appointed operators within their established authority. A Transaction Specification shall identify the permitted roles, actions, and sources; the descriptions above do not independently grant access to information or authority to act.

(c) An Open Access designation covers the stated exchange and the included functions established in Exhibit A. It does not require SHN to perform the substantive work of the source institution or supply a separately commissioned analytical result or coordinated workflow.

4. Individual Visibility and Member Services.

Entitled transaction evidence and authorized source updates may be made available through Member Services, Participant applications, and qualified third-party applications in accordance with Section 5 of the Network Rules.

For example, a prior-authorization tracker may present submission and receipt events, source status and decisions, requests for additional information, and available next actions. Presentation of that information does not require a separate institutional Transaction Type. A request or action taken through the service shall follow the applicable Transaction Specification and authority.

5. Additional Results and Coordinated Services.

SHN may separately offer Network Management, Network Intelligence, and Network Orchestration under Exhibit A and applicable Service Orders. Such services may use the Open Access Transactions listed above without changing their fee designation.

For example, exchanging existing source information is within the applicable Open Access scope above. A separately commissioned service that combines authorized contributions from multiple sources to produce an additional analytical result or coordinate resulting actions may be offered as Network Intelligence or Network Orchestration.

Any additional Catalog entry for such an offering shall identify the purchased work and applicable fee reference. This Section does not itself establish a product, price, or production-availability commitment.

EXHIBIT C: BASE SERVICE LEVEL AGREEMENT

This Service Level Agreement ("SLA") forms part of the Network Rules and applies to the common Network services SHN provides without a service fee ("Base Services"). Capitalized terms not defined here have the meanings given in the Network Rules or the applicable Network Participation Agreement ("Agreement").

1. Covered Services

1.1 Scope. Base Services comprise the SHN-operated Hub and its required authentication, control-checking, and encrypted-routing dependencies; Network Trust Services; and the common interfaces and evidence-access functions SHN is required to provide under the Network Rules, including applicable status, receipt, and Audit Log access. This SLA applies to supported production functions within their published scope. Network Trust Services applicable to participation do not depend on a Gateway deployment, Hub use, or purchase of an Additional Service.

1.2 Operating boundary. SHN is responsible for the covered functions it operates, including work performed on its behalf by suppliers. Qualification of a non-Hub Qualified Transaction Path does not make SHN its operator or excuse the path's required evidence, retention, and access without charge; those remain qualification conditions governed by the lawful retention and access arrangements established under Section 7.8(d) of the Network Rules. This SLA does not promise availability of Participant-operated systems, independently operated Gateways or paths, or source systems, or completion of a counterparty's clinical, coverage, payment, or other business decision.

1.3 Separate services. Gateway Management, Enhanced Support, and other Additional Services are governed by their applicable Service Orders and separate service terms. This SLA does not include operating a Participant's environment, custom integration, configuration assistance, or troubleshooting unrelated systems. Individual rights and Member Services remain governed by the Network Rules and applicable Member Terms; this SLA covers SHN's required common access functions without creating a performance commitment for every Member application or service.

2. Availability and Common Performance

2.1 Hub availability objective. SHN shall use commercially reasonable efforts to make the covered production Hub functions available at least 99.9% of each calendar month, calculated under Section 3. This is an availability objective, not a guaranteed numerical minimum or a promise of uninterrupted or error-free operation. A shortfall does not, by itself, establish breach of a guaranteed result, but does not excuse SHN's efforts, incident-handling, reporting, or corrective duties.

2.2 Network Trust Services. SHN shall operate Network Trust Services in accordance with the Network Rules and published operating requirements identifying the covered functions, verification scope, evidence currency, correction process, and change-propagation

requirements. Responses shall distinguish verified information from source assertions and identify relevant limitations or unresolved status. SHN shall apply applicable revocations and corrections within the requirements for the affected function. An appropriately unresolved result is not itself an outage; a failure to perform SHN's assigned work remains subject to investigation and correction.

2.3 Required interfaces and evidence. SHN shall maintain the supported common interfaces for required status, receipt, and Audit Log access and use commercially reasonable efforts to restore them when unavailable. A failure of these functions remains a Base Service incident even if it does not interrupt Hub routing. Entitled access and required correction shall not depend on purchase of support or an archival service. Retention, Individual access, and information-handling duties remain as specified in the Network Rules. A receipt, Hub acceptance, and source decision are distinct events. Transport events do not independently establish or alter a legal or contractual deadline; their legal effect, and that of source decisions, is governed by applicable law and expressly accepted arrangements. A retry does not itself create a new business request or restart a deadline. Model output is not the sender's assertion.

2.4 Published operating requirements. SHN shall publish the supported production boundaries, capacity and message limits, functional timeouts, safe refusal and retry behavior, and relevant monitoring and incident channels. Requirements may vary with the supported function and implementation and shall apply consistently to comparable scope. They shall be identified before the affected function is activated. Technical specifications may explain these requirements but may not amend this SLA or protected Network obligations without the applicable amendment process.

3. Measurement and Reporting

3.1 Availability calculation. Monthly Hub availability equals 100 × (Eligible Minutes − Downtime Minutes) ÷ Eligible Minutes. Eligible Minutes are the minutes in the applicable production-service period during the calendar month, less permitted maintenance and exclusion minutes under Section 4. Each minute shall be counted or deducted only once. A period with no Eligible Minutes shall be reported as not applicable.

3.2 Downtime. Downtime means the covered Hub function is unavailable at its published production boundary, including failure to accept and perform required controls and routing for conforming, authorized requests within the applicable functional timeout. Correct refusals are not Downtime. Increased latency within that timeout, or failure solely of a recipient or source system, is not Hub Downtime. Failure of a required SHN-operated dependency counts when it prevents the covered function. SHN shall identify materially affected boundaries or functions rather than conceal their failure through a Network-wide average. Downtime Minutes are the Eligible Minutes during which Downtime occurs.

3.3 Evidence and reporting. SHN's monitoring shall be the primary measurement source. SHN shall reasonably consider credible Participant evidence, correct demonstrated errors, and identify material monitoring gaps or unresolved attribution. SHN shall make a monthly

performance summary available through a common reporting channel within ten (10) Business Days after the end of each calendar month, identifying measured availability, material incidents, actual unavailability before deductions, maintenance and other exclusions, and corrective status. A common report may serve affected Participants, supplemented where needed to explain their affected scope. Participants may raise supported measurement objections through the designated operational contact; SHN shall investigate and provide a reasoned response. Required incident notices shall not await the monthly report.

4. Maintenance and Exclusions

4.1 Planned maintenance. SHN shall use commercially reasonable efforts to perform maintenance without interrupting Base Services. For planned disruptive maintenance, SHN shall give at least forty-eight (48) hours' advance notice identifying the affected functions, start time, and expected duration. Only actual unavailability within the notified period may be excluded, subject to an aggregate maximum of two (2) hours per calendar month. Excess time counts as Downtime unless independently excluded under this Section.

4.2 Emergency maintenance. SHN may perform emergency maintenance when reasonably necessary to prevent imminent material harm or comply with a binding legal obligation. SHN shall provide notice as soon as practicable and record the reason, affected scope, and duration. Only time reasonably necessary for the emergency work may be excluded. A preceding outage does not become excluded merely because emergency maintenance follows it.

4.3 Other exclusions. Unavailability may be excluded only to the extent and for the period directly caused by: (a) a Participant's misuse or failure to comply with applicable requirements, including a required update after its permitted implementation period; (b) failure of independently operated systems or communications outside SHN's covered service; (c) an agreed suspension of the affected connection or a restriction properly imposed under the Network Rules; or (d) a force majeure event qualifying under the Agreement. Expressly designated non-production features are outside the availability objective, but their involvement does not exclude failure of a separate production function.

4.4 Limits on exclusions. SHN shall reasonably document the causal basis and duration of an exclusion. Supplier failure or a cyberattack is not automatically excluded; SHN remains responsible for its assigned safeguards and recovery duties. Exclusions do not excuse security notices, mitigation, required evidence access, or other independently applicable obligations. Unresolved causation shall be identified as unresolved rather than automatically treated as an exclusion.

5. Base Incident Handling

5.1 Reporting and triage. SHN shall maintain an incident-reporting channel available at all times and publish operational and security escalation contacts. Continuous submission does not itself promise continuous live-agent support. SHN shall maintain an on-call escalation arrangement for critical Base Service incidents requiring urgent protection or restoration. Reports need only identify the affected function and observed problem to the reporter's reasonable knowledge.

SHN shall assess credible reports and determine whether they concern a Base Service failure without requiring a support purchase. Participants shall not delay reporting a suspected security incident, material Base Service outage or risk to other Participants while completing troubleshooting. SHN shall route a misdirected incident report to the responsible internal team without requiring resubmission or restarting the applicable response clock.

5.2 Response and updates. SHN shall prioritize common-service incidents by severity and actual impact. Purchase of Enhanced Support or another Additional Service shall not confer priority in assessing or restoring common services, including among equally urgent incidents. Dedicated communications and assistance may be provided within the separately purchased scope without delaying required common-incident handling. SHN shall reasonably assign severity based on that impact and explain any reclassification to the reporting Participant. Critical incidents involving loss of a core production function without a reasonable workaround, or an active material security or information-exposure risk, shall receive prompt assessment, appropriate escalation, and continuing restoration or protective efforts. SHN shall provide affected Participants timely status updates as material information becomes available, using a common incident channel where appropriate. Less urgent defects and routine inquiries shall remain on the included ordinary support channel. An automated receipt is not a substantive assessment. SHN shall use commercially reasonable efforts to provide a substantive assessment of a critical Base Service incident within thirty (30) minutes after SHN's detection or receipt of a credible report, whichever occurs first, at all hours; restoration remains subject to commercially reasonable efforts, without a guaranteed resolution deadline, and independently applicable notice deadlines remain effective.

5.3 Cooperation and scope. Participants shall provide reasonably available, appropriately minimized technical information and cooperate with investigation. Ordinary tickets shall not include healthcare payloads, private keys, or credentials; necessary sensitive diagnostics shall use an authorized secure channel. SHN shall identify work outside Base Services and obtain agreement before charging for optional assistance. Correction of SHN's common-service defects shall not depend on purchasing that assistance.

6. Correction, Escalation, and Remedies

6.1 Restoration and corrective action. For a material Base Service failure, SHN shall promptly investigate, mitigate, and use commercially reasonable efforts to restore the affected function. SHN shall document corrective actions, accountable owners, and expected milestones, and provide an appropriate summary to affected Participants. Recurring material failures shall receive senior operational review and a plan addressing recurrence. A common plan may serve multiple affected Participants. Investigation or preparation of a report shall not delay necessary protective or restoration work. The same material shortfall against the Hub availability objective in two consecutive calendar months requires SHN to deliver the corrective-action plan to affected Participants within ten (10) Business Days after the end of the second such month; failure to deliver the required plan within that period constitutes a breach of the correction duty.

6.2 Remedies. If the covered Hub service used by a Participant experiences material shortfalls against the availability objective in three consecutive calendar months, calculated under Sections 3 and 4, that Participant may terminate its Network Participation Agreement immediately by written notice to SHN, without establishing fault or breach, observing the ordinary termination notice period, or paying an early-termination penalty. Accrued obligations and required transition, records-access, information-handling, and other surviving duties remain effective. Time-based service credits are available under Section 6.4. Applicable rights concerning breach, correction, escalation, termination, records access, and transition remain governed by the Agreement and Network Rules. Liability, damages, indemnification, insurance, and incident-cost allocation remain governed by the applicable agreements. This SLA neither creates a new liability cap nor makes a service-level remedy exclusive.

6.3 Continuing duties and changes. Security, privacy, Individual rights, evidence retention, and continuity obligations apply independently of the availability objective and any exclusion. Changes to this SLA follow the amendment provisions of the Network Rules and Agreement. Changes to monitoring tools or reporting format shall operate prospectively, apply consistently, and shall not retroactively remove an outage or materially reduce the stated commitment without the required amendment process.

6.4 Time-based service credits. For each calendar month, an affected Participant shall receive a credit in minutes equal to the greater of zero or its Downtime Minutes minus 0.1% of its Eligible Minutes, calculated under Sections 3 and 4. SHN shall record the credit with the monthly performance summary and correct it for verified measurement errors. Overlapping Downtime counts once per Participant, regardless of the number of affected functions, connections or Transactions.

The Participant may redeem the credit within twelve (12) months after it is recorded against one recurring paid SHN service it purchases under a Service Order, whether already purchased or purchased during that period. The invoice reduction equals the agreed recurring fee for the applicable billing period multiplied by credited minutes redeemed and divided by the total minutes in that billing period, and shall not exceed that period's recurring fee. Unused minutes remain available until expiry. Credits have no cash or transfer value, do not apply to one-time charges, usage-based charges, taxes or external-cost pass-throughs, and may be redeemed only once. For the same outage, the Participant may use this credit or a credit under the purchased service's terms, whichever is greater, without stacking them. No purchase is required to retain participation or Open Access rights. Credits do not replace correction duties, the exit right under Section 6.2 or other applicable remedies; duplicate recovery for the same loss is not permitted. Credits under this Section are noncash adjustments to charges for an eligible purchased service. They do not count toward or increase the monetary liability limits under the Network Participation Agreement and do not alter the treatment of any separate claim under that Agreement.

Initial Transaction Specification: Prior Authorization

Smart Health Network | Version 1.0 | Oct 7, 2026

Effective date: As stated in the applicable adoption notice.

Transaction Catalog entry: Prior Authorization | Geographic scope: United States

This Specification establishes the SHN exchange requirements for United States medical prior authorization using the HL7 Da Vinci Coverage Requirements Discovery (CRD), Documentation Templates and Rules (DTR), and Prior Authorization Support (PAS) implementation guides. It supports implementation of the CMS Prior Authorization API requirements.

Scope and governing terms

This Specification applies to prior authorization for medical items and services, excluding drugs, within each Participant's accepted and activated scope. It covers requirements discovery, documentation, submission, status inquiry, additional information, decisions, updates and cancellation as supported by the applicable guides. Appeals, claims adjudication and drug prior authorization are outside this version.

This initial Transaction Specification is issued under the Network Rules and applies to each Participant's accepted Prior Authorization roles and scope. It is included with the Rules for circulation and remains separately versioned. Changes follow Rules Sections 3.2(f) and 6.6, including applicable approval, notice, qualification and transition requirements. Its inclusion does not itself activate a connection or make each Specification update an amendment to the Network Rules or standard Network Participation Agreement.

The Network Rules, Network Participation Agreement and applicable processing terms govern participation, authority, security, evidence, retention, fees, service levels and liability. The designated Open Access exchange and required status exchange do not require purchase of an Additional Service. The payer remains responsible for coverage determinations, required notices and applicable decision deadlines; the submitting party remains responsible for information it supplies. Network participation or technical conformance alone does not establish regulatory compliance.

Standards and versions

Implementations shall use FHIR R4 (4.0.1) and conform to the applicable requirements of the following Da Vinci Implementation Guides for their supported roles. Eligible version families include 2.0, 2.1 and 2.2. Production support is limited to the exact versions, dependencies, roles and combinations identified as qualified in SHN's current compatibility record.

Guide	Version families	Function
CRD	2.0, 2.1 and 2.2	Discover prior authorization and documentation requirements.
DTR	2.0, 2.1 and 2.2	Obtain and complete payer documentation templates and rules.
PAS	2.0, 2.1 and 2.2	Submit, inquire about, update and cancel requests; exchange responses and decisions.

SHN shall maintain a published compatibility record identifying the exact qualified guide versions, required dependencies, supported roles and operations, and production availability. Dependencies include the applicable US Core, SMART authorization, CDS Hooks and questionnaire standards required by the selected guides and law. The record shall distinguish testing from production support.

Participants may qualify using eligible 2.0, 2.1 or 2.2 releases appropriate to their implementation and applicable legal requirements. Endpoints shall declare their supported capabilities. Each activated connection shall use an expressly qualified combination of guide versions and dependencies; a shared major version does not establish interoperability. Unsupported combinations shall be rejected clearly, without silent downgrade or loss of information. Additional versions require qualification and notice under the Rules before production use.

Exchange and responsibilities

Providers and their authorized submitters shall use the applicable CRD and DTR functions to obtain requirements and assemble documentation, and PAS to exchange authorization requests and responses with the payer or its authorized delegate. Each party shall implement the guide requirements assigned to its role. A PAS submission need not repeat discovery or documentation work already validly completed.

Hub exchanges require qualified Participant Gateway functionality, which may be self-operated, shared or supplied by a qualified operator. Gateways shall preserve the guides' payloads, identifiers, operation semantics and responses through the qualified transport binding. Any

translation shall preserve meaning and be identified and validated during qualification. The Hub shall route encrypted Messages without reading their substantive content.

Each party shall establish the legal authority required for its role and disclosures, including any consent required by applicable law. This Specification imposes no additional Individual consent requirement for the provider-payer PA exchange. Delegates act within their established authority.

The payer shall return the applicable approval, denial or request for additional information, including authorization details and expiration, specific denial reasons, or the information needed, as applicable. Responses shall preserve service-line outcomes, quantities, periods and mixed decisions where relevant. This Specification adopts the guides' resources and codes; it creates no separate SHN clinical or authorization-status vocabulary.

Individual access and request-status tracker

Individuals may access Hub Metadata concerning their PA exchanges under Rules Sections 5.2 and 7.8, subject to applicable verification and information protections. SHN provides that access through the supported interfaces and qualified applications described in the Rules. This access does not depend on tracker availability.

Status presentation. PA status information exchanged under this Specification may be presented through SHN, Participant or integrated applications where the applicable service is established. Additional requirements for status delivery, presentation and notifications shall follow the applicable Specification amendment process. Any additional Participant roles or scope shall be expressly accepted in its Transaction Schedule and qualified before activation.

Receipt and continuity

Implementations shall distinguish transport acknowledgment, recipient receipt, payer acceptance for processing and payer determination. Applicable law determines the effect of those events on decision deadlines. A network status label does not postpone a legally effective receipt date.

Implementations shall preserve urgent or expedited designations through submission, routing, status updates and retries. Any authorized change shall remain attributable and visible in the request history. Requests, responses and service lines shall retain the identifiers needed for correlation from initial submission. Retries shall be recognizable as retries and shall not create duplicate business requests or restart a decision clock. After a lost acknowledgment or timeout, the parties shall reconcile status before treating a retransmission as a new request. Corrections shall remain linked to the prior record.

Endpoints shall communicate actionable validation and delivery errors and support an identified escalation and fallback process for outages or unresolved outcomes. A path or operator change shall preserve request identity, known status and records needed for continued processing. Required legal deadlines and notices remain applicable during a technical failure.

Qualification and activation

Before activation, SHN and the responsible Participants or operators shall record the roles, endpoints, guide versions and dependencies, Gateway transport binding, authorization configuration, status-update mechanism, operational contacts and supported scope. The binding shall document routing, request and response correlation, errors and timeouts without changing the guides' business semantics. Necessary processing, retention and access arrangements shall be in place under the Rules.

Qualification shall demonstrate the applicable CRD, DTR and PAS workflow end to end, including approval, denial, additional-information exchange and status inquiry. Testing shall also cover mixed service-line outcomes, invalid or unauthorized submissions, unsupported versions, duplicate delivery, lost acknowledgments, updates or cancellation, and outage recovery where applicable to the activated role. SHN may rely on sufficient current conformance evidence and limit additional testing to the Network integration and unresolved risks.

The responsible endpoints shall retain the business records and status evidence assigned to them. The Hub Audit Log shall contain only the permitted Network Metadata under the Rules. Publication of this Specification or a Catalog entry does not establish production readiness or activate a Participant.

Informational regulatory and standards references (non-normative)

As of Oct 7, 2026, CMS-0057-F requires a standards-based Prior Authorization API and recommends the Da Vinci guides. This Specification requires conformance to the applicable guides using the versions identified in the compatibility record. ONC adopted CRD 2.2.1, DTR 2.2.0 and PAS 2.2.1 effective Oct 1, 2026; that standards adoption is distinct from CMS's proposed requirement to mandate the guides for payers under CMS-0062-P. Proposed drug requirements are not included here.

FHIR-only exchange may rely on applicable CMS enforcement discretion concerning X12 278. This Specification grants no exception from law or third-party licensing requirements. A use outside that discretion requires an independently lawful implementation.

CMS API standards and implementation guides

ONC adopted standards effective Oct 1, 2026

Da Vinci CRD 2.2.1

Da Vinci DTR 2.2.0

Da Vinci PAS 2.2.1