

MASTER USE CASE AGREEMENT

This Master Use Case Agreement (“**Master Use Case Agreement**” or “**MUCA**”) governs your organization’s participation in Use Cases. Your organization is referred to as a “**Participant**” in this Master Use Case Agreement. By accepting these terms, you are agreeing that this Master Use Case Agreement is effective and binding upon Participant, and subject to the Terms of Service (the “**Agreement**”) between the Participant and the [ENTITY] (“**Network**”). Network and Participant are referred to herein collectively as “**Parties**” and individually as a “**Party**.”

1. Purpose.

1.1. The purpose of this Master Use Case Agreement is to set forth the requirements for Participant to participate in Use Cases and Pilot Activities.

1.2. Use Cases: To enter into a Use Case, Participant must review and accept the terms surrounding a specific Use Case. The terms of a specific Use Case are set forth in a “**Use Case Exhibit**” or “**UCE**” and, upon acceptance, each Use Case Exhibit is subject to the terms of this Master Use Case Agreement and incorporated herein by reference.

1.3. Pilot Activities: To enter into a Pilot Activity, Participant must review and accept the terms surround that Pilot Activity. The terms of a specific Pilot Activity are set forth in a “**Pilot Activity Exhibit**” or “**PAE**” and, upon acceptance, each Pilot Activity Exhibit is subject to the terms of this Master Use Case Agreement incorporated herein by reference.

2. **Use Case Diagrams.** Each Exhibit may include a diagram setting forth the anticipated flow of Message Content.

3. **Definitions.** Capitalized terms used in this MUCA and not otherwise defined herein are available at: www.velatura.org/emuca-definitions/, as may be modified from time to time, the terms of which are incorporated herein by reference.

4. **Message Content.** Participant and Network shall only send, receive, find or use Message Content pursuant to each Use Case as follows:

4.1. **Primary Use** Message Content and related Notices are used during the term of an Exhibit and only for the use(s) set forth in that Exhibit.

4.2. **Additional Permissible Use** This section sets forth additional permissible uses that apply to many, but not all, Use Cases. Each Exhibit specifically identifies which of the below additional permissible uses *do not* apply to that Use Case in the corresponding section 4.2 of the Exhibit.

4.2.1. TPO. Message Content may be used by Health Providers for Treatment, Payment and/or Healthcare Operations consistent with the requirements set forth in HIPAA;

4.2.2. Public Health. Message Content may be used for public health activities and reporting as permitted by Applicable Laws and Standards;

4.2.3. Federal Programs. Message Content may be used as required by Federal Programs.

4.2.4. Individual Authorization. Message Content may be used and disclosed pursuant to an authorization provided by the individual who is the subject of the Message Content or such individual's personal representative in accordance with Applicable Laws and Standards;

4.2.5. Archiving. Message Content may be archived by Network for audit, trending, and quality control purposes.

4.2.6. Use Case Enablement. Message Content may be used in other Use Cases only if Participant enters into other UCEs that require Message Content from that Use Case.

4.2.7. Pilot Activities. Message Content may be used by Participant or Network subject to a mutually agreed Pilot Activity Exhibit (PAE) developed under a formally approved pilot project, provided that such purposes are mutually agreed upon and consistent with Applicable Laws and Standard. Pilot approval shall be obtained either from the Network Board of Directors or the Use Case working group. This provision will be deleted by most UCEs.

4.2.8. Enrichment. Message Content may be enriched by Network for the purpose of standardizing and simplifying the ability of other TDSOs that receive the data to use it. This may include appending additional information (e.g. a risk score) to enhance and streamline automated processing by receivers of enriched Message Content.

4.2.9. Participant Usage of Message Content. Subject to any restrictions or limitations on use set forth in any Exhibit or Use Case Agreement executed by Participant, Participant may use Message Content in accordance with the terms of any agreements or authorizations in place between Participant and its Authorized Users, provided that such Authorized Users have the full rights and authority to grant the applicable rights.

4.2.10. Participant and Network may send, receive, find, and use Message Content for "Individual Access" and "Benefits Determination" as those terms are defined in the most recent version of the Trusted Exchange Framework and Common Agreement as published in the Federal Register. Prior to publication of the Trusted Exchange Framework and Common Agreement in the Federal Register, those terms shall have the meaning set forth in the Draft Trusted Exchange Framework published by the Office of the National Coordinator for Health Information Technology on January 5, 2018.

4.3. **Limitations on Use** The applicable Exhibit will set forth any additional limitations on use of Message Content.

4.4. **Pilot Activity Use** Message Content sent, received, found or used pursuant to each Pilot Activity Exhibit shall only be used during the term of the Pilot Activity Exhibit and only for the development of future Use Cases as further set forth in each Pilot Activity Exhibit.

4.5. **Related Use Case Requirements** Certain Use Cases may require Participant to enter into other Use Cases. These Use Cases are interdependent to fully support each Use Case. Each Exhibit will set forth any such requirements. Organizations participating in any Exhibit will

need to also participate in the [Common Key Service Use Case and the Active Care Relationship Service Use Case] unless an Exhibit specifically excludes participation in the CKS or the ACRS Use Cases.

Commented [A1]: States may want to insert their own additional related Use Cases here

5. Fees.

5.1. Fees, if any, related to any Use Case will be included in a separate Statement of Work (“SOW”) mutually agreed to by Network and the Participant. Either Party may terminate, upon ninety (90) days’ prior written notice, its participation in this Master Use Case Agreement or any Exhibit for a failure by the other Party to pay any undisputed fees when due according to a mutually agreed upon SOW. If the non-paying Party remedies the non-payment during the ninety-day notice period, participation will not be terminated.

6. **Service Level.** The Parties desire that the Message Content and Notice exchange between Participant and Network meet the service levels set forth below:

6.1. **Timeliness of Exchange** The Parties agree that the Message Content and Notice exchange shall occur on a Transactional Basis unless otherwise required by an Exhibit.

6.2. **Queued Messages** Notwithstanding Section 6.1 and Transactional Basis, if the Parties experience a Service Interruption, then Message Content and Notices queued during the Service Interruption shall be retransmitted as soon as practicable upon such Service Interruption ending. Unless specified otherwise in an Exhibit, Network may queue Message Content and Notices for up to ninety-one (91) days.

6.3. **Service Interruptions** The Parties agree to notify each other of any scheduled or unscheduled Service Interruption in accordance with the procedure available at: www.velatura.org/service-interruptions (the “**Service Interruption Procedure**”).

7. Auditing.

7.1. **Abilities to Audit** The Parties shall monitor and audit all access to and use of their respective systems related to this MUCA, for system administration, security, regulatory compliance and other legitimate purposes consistent with each Party’s respective standard operating procedures.

7.2. **Audit Logs**

7.2.1. Participant Participant shall log the following information: (i) date and time Message Content was accessed and the identity (*e.g.*, unique identifier) of the individual or system, as applicable, accessing the Message Content; (ii) date and time Message Content was sent to the Services and the identity of the individual or system, as applicable, sending the Message Content; (iii) date and time a Notice was sent or received from or to the Services; (iv) the unique message identifier for the Message Content accessed, sent, or received; (v) the Message Content accessed; and (vi) any Notices, failures, or network events.

7.2.2. Network Network shall log the following information: (i) name of Participant and any Authorized Users accessing the Services; (ii) the identity (*e.g.*, unique

identifier) of the individual or system, if applicable, accessing the Message Content; **(iii)** the date and time the access occurred; **(iv)** the Message Content accessed; **(v)** a description of Message Content accessed; and **(v)** any Notices, failures, or network events. Except as provided in the immediately preceding sentence, Network shall not be obligated to maintain and shall not be responsible for, either maintaining records of Message Content exchange between the Parties or inspecting Message Content

7.3. **Production of Audit Logs** Upon a good faith written request by a Party, the other Party shall either: **(i)** produce the requested audit logs within five (5) business days; or **(ii)** provide to the other Party a reason why it is unable to produce such audit logs within five (5) business days and an estimate as to when such audit logs will be provided.

7.4. **Retention of Audit Logs** The Parties shall retain audit logs in accordance with Applicable Laws and Standards and in all cases for at least thirty (30) days.

8. Responsibilities of the Parties.

8.1. Participant's Responsibilities

8.1.1. Resending For Exhibits where Participant is sending Message Content to the Services, or using the Services to query to find Message Content, Participant shall resend, or make provisions to have resent, queries, Notices, and Message Content, as applicable, to the Services, which **(i)** Participant failed to successfully send to the Services, or **(ii)** Network failed to successfully send to a TDSO, upon Participant receiving a failure Notice from the Services so long as the Services does not send such failure Notice after having first acknowledged and accepted with no errors the message from Participant. In the event a query to find Message Content is no longer needed by the Participant, the retransmission may be done at Participant's option.

8.1.2. Notices For Exhibits where Participant is sending Message Content to the Services, or using the Services to query to find Message Content, Participant shall, on a Transactional Basis, send any Notices received from the Services to the Authorized User that sent the query or Message Content (e.g., sending an acknowledgment of submission received from the Services). In cases where sending the Notices to the Authorized User's system would cause undue harm, this requirement can be waived on a case by case basis and with written approval from Network. The specifications for the Notices and Message Content are set forth on the Network web site in the Use Case Implementation Guide for the applicable Exhibit.

8.1.3. Validation and Conformance For Exhibits where Participant is sending Message Content to the Services, or using the Services to query to find Message Content, Participant shall validate the query or Message Content to ensure that it **(i)** is properly addressed with both sender and receiving facility; **(ii)** includes the purpose of use; and **(iii)** conforms to the Use Case Implementation Guide and other specifications which may be set forth in each Exhibit.

8.1.4. Sending For Exhibits where Participant is sending Message Content to the Services, or using the Services to query to find Message Content, Participant shall send to the Services the query or Message Content that **(i)** is properly addressed with both sender and receiving facility; **(ii)** includes the purpose of use; and **(iii)** conforms to the Use Case Implementation Guide and other specifications which may be set forth in each Exhibit.

8.1.5. Authorized User Compliance For all Use Cases involving the Services, Participant shall send, receive, find or use Message Content only with Authorized Users that have agreed to abide by the applicable terms of this Master Use Case Agreement and the corresponding Exhibit(s). Participant shall bear sole responsibility for ensuring that any Message Content sent to the Services meets the data integrity, format, security, and timeliness standards prescribed by the applicable Exhibit. Participant is responsible for ensuring compliance with this MUCA and the applicable Exhibit(s) by its Authorized Users and as between Network and Participant, shall remain fully liable for the acts or omissions of its Authorized Users.

8.1.6. Unauthorized Message Content In the event Participant sends, receives, finds or uses Message Content for which Participant is not authorized to send, receive, find or use, Participant will promptly upon discovery inform Network, delete such Message Content, and require its Authorized Users to delete such Message Content as well.

8.1.7. Change Coordination Participant shall reasonably cooperate with Network to schedule and coordinate any changes to the production systems or networks involved in sending, filtering, translating, forwarding, finding or receiving Message Content so as to ensure the reliability and availability of the production environments according to the Service Interruption Procedure.

8.1.8. Troubleshooting and Support Participant is responsible for the initial troubleshooting and support for its Authorized Users. If Participant cannot resolve a trouble with a Authorized User, Participant will report the trouble as specified by the Service Interruption Procedure.

8.1.9. Patient Consent Participant agrees that when it sends, receives, finds or uses Message Content Participant will practice consent management and comply with Applicable Laws and Standards. This process enables all parties to determine what Patient Data can be accessed at various points of care. By way of example, if an Exhibit specifies sending Health Information that may not be sent without patient consent under HIPAA or SAMHSA rules, Participant must not send any Message Content or Patient Data containing Health Information for which an express patient authorization or consent is required (e.g., mental or behavioral Health Information) without first confirming that a valid patient consent exists and permits Patient Data to be sent only to the receiving Health Provider(s) named by the patient on the consent.

8.1.10. Data at Rest If Participant or Authorized User determines, after conducting a risk assessment and in accordance with HIPAA, that encryption of data at rest is commercially reasonable and appropriate for Message Content, then Participant or Authorized User shall encrypt Message Content while at rest in any Participant Source System(s).

8.1.11. Acknowledgements and Negative Acknowledgments If an applicable Use Case employs ACKS /NACKs, and Participant receives any NACKs for that Use Case, it: **(i)** will act upon all ACKS/NACKs; **(ii)** will take any necessary corrective action based on ACKS/NACKs; and **(iii)** will send ACKS/NACKs directly back to the Authorized User or take responsibility for communication and correction.

8.1.12. Secure Transport Participant shall send, receive, find or use the Message Content and Notices using one of the Network approved secure transport methods, format and content.

8.1.13. Electronic Addresses If the applicable Use Case involves sending, receiving or finding Message Content, then Participant and its Authorized Users shall provide and maintain correct Electronic Addresses and Electronic Service Information (ESI) with Network.

8.1.14. Privacy Tags If required by the Network Board, the sender of any Message Content that contains Specially Protected Information must include special machine readable Privacy Tags in the Message Content as specified in the Use Case Implementation Guide. If Message Content contains any Privacy Tags, the sending Participant must confirm that patient has consented to recipient receiving the Message Content before Participant sends the Message Content.

8.2. Network's Responsibilities

8.2.1. Network Data Sharing Network shall send, receive, find or use Message Content and Notices with Participant and with other TDSOs and on a Transactional Basis as applicable for each Exhibit.

8.2.2. Confidentiality and Security Network shall use commercially reasonable efforts to protect the confidentiality and security of Message Content for so long as such Message Content is under the control of Network.

8.2.3. Change Coordination Network shall reasonably cooperate with Participant to schedule and coordinate any changes to the production systems or networks involved in Message Content sending, filtering, translating, forwarding, finding or receiving activities so as to ensure the reliability and availability of the production environments according to the Service Interruption Procedure.

8.2.4. Network and TDSO Compliance Network shall send, receive, find or use Participant Message Content only with other TDSOs that have agreed to abide by the applicable terms of this Master Use Case Agreement and the corresponding Exhibit(s).

8.2.5. Secure Transport Network shall send, receive, find or use the Message Content and Notices using one of the Network approved secure transport methods, format and content.

9. General Terms.

9.1. Data Format, Validation and Transmission Specifications

9.1.1. The Message Content sent to the Services will be set forth in the Exhibit or will be determined during the Pilot Activity. A Use Case Implementation Guide for each Exhibit will specify the Conforming Message for each data sharing scenario set forth in the Exhibit. All Message Content sent to the Services shall meet these specifications. As applicable, a Use Case Implementation Guide for the Use Case being piloted may still be undergoing revisions but should

be finalized during the Pilot Activity and will specify the Conforming Message for each data sharing scenario set forth in the Pilot Activity Exhibit.

9.1.2. Network shall optionally validate all Conforming Messages.

9.2. **Pilot Activity Message Content** Upon termination or expiration of a Pilot Activity Exhibit, Participant shall delete and render unrecoverable and unreadable all Message Content from the Pilot Activity from all storage locations.

9.3. **Notice** Any requirements in this MUCA for written notice may be satisfied through email notification in accordance with the Agreement.

9.4. **Additional Terms** The Parties may set forth additional terms applicable to a specific Use Case or Pilot Activity in each Exhibit, respectively.

9.5. **Order of Precedence** Upon execution by both Parties, an Exhibit shall supersede and replace any other version of the Exhibit for that Use Case previously executed between the Parties. To the extent there is a conflict between the terms of an Exhibit, the terms of this MUCA, and/or the Terms of Service, the terms of the Exhibit, as applicable, shall control over the MUCA and the terms of the MUCA shall control over the Terms of Service. When a Pilot Activity period ends, all terms in the Pilot Activity Exhibit expire and a Use Case Exhibit shall be agreed to by the Parties to move from pilot status into production status for the Use Case.