CT DPH will require this Collaboration Protocol Agreement (CPA) from all external partners who will be sending public health reporting.

Steps:

1. CT DPH and external entity have a discussion about using CDC's PHIN MS as the transport mechanisms. The external entity that can be a provider or organization for multiple providers or EHR vendors that plan on sending data via their centralized hub for their clients

2. CT DPH will send e-mail request to CDC's PHIN MS Support group with external entity on copy requesting that the message exchange is being requested. CT DPH has its CPA completed since 2010 and is completely set up with sender and receiver. A Collaboration Protocol Agreement (CPA) is a business-level agreement between the PHINMS Sender and Receiver. The CPA stores information necessary for partners to communicate with one another. It includes the transport protocol and security constraints both partners have agreed to use when messaging one another. A CPA is required for each location which has installed PHINMS. The CPA file name consists of the Receiver's and Sender's PartyID with an .xml extension. The file is stored in both the PHINMS Receiver's CPA directory and the Sender's CPA directory.

3. External entity works with CDC PHIN MS Support group on CPA, generation of their PartyID, digital certificate from the Secure Data Network (SDN), requesting the ability to send messages to production and testing SDN and installation of PHIN MS and configuration of their sender and receiver. See the link PHIN MS Collaboration Protocol Agreement Guide v1.0.0

4. After installation and configuration is complete, external entity contacts CT DPH for CPA and public portion of digital certificate for encryptions and CT DPH send its information for building connection and agreeing to PHIN MS route information and a connectivity test is performed for both test and production within PHIN MS.

These steps are after there has been a vendor agreement signed to use PHIN MS with DPH:

For routes where the RNR is not available we will need to handle several other issues.

- Exchange the PHINMS CPA routing files.
    - The PHINMS CPA routing files are XML files based on the route maps for senders, and are the first level of authentication after the message has reached the PHINMS receiver. The public key certificate mapping would already have been validated by this point. For one directional flow we would only need to import the sender's CPA routing file. For bi-directional we would also need to send our CPA routing file to the receiver for them to import into PHINMS.
- Define the sets of service/action pairs.
    - These provide the next level of validation. Only messages that have a service/action pair mapped to a work group will be consumed and persisted to the database. The RNR handles this by using a common service/action pair for all RNR routing.