

# **eHHR Enhanced Memorandum of Understanding (E-MOU)**

## **Appendices**

## **Preface to Appendices**

In any Data Exchange Service there are two distinct entities: a Publisher and one or more Subscribers. The Publisher is the entity that discloses data to another Partner. The Subscriber is the partner (or partners) that receives data from the Publisher. While the two entities need to work together to determine the terms of the data sharing, they have distinct roles in onboarding a Data Exchange Service to the E-MOU. In general these are their responsibilities related to onboarding:

### **Publisher Role:**

- Describe the service available and the requirements for onboarding using Attachment A: Publisher Requirements for Data Exchange Services
- Work with Subscriber Applicants and the Coordinating Committee to answer questions and support onboarding when a Subscriber Applicant is approved to begin testing to onboard to a Data Exchange Service.

### **Subscriber Role:**

- Review what Data Exchange Services are available. When a service is of interest, complete Attachment B: Subscriber Requirements Template for Data Exchange Services.
- Work with Publisher and Coordinating Committee to answer questions and complete testing and onboarding when approved to receive a Data Exchange service. These parties will work together to ensure terms allowing access to the published data are complied with by the Subscribing Partner.

There are two types of services within the Data Exchange, those being Electronic Data Interchange (EDI) and Extract, Transform, Load (ETL) Services. While technically implemented differently, these Data Exchange Services have more business similarities than differences and so they are treated in the E-MOU under a common framework. Below are examples of Data Exchange Services:

### **Examples Services:**

- A secure web service that validates real-time if a Citizen is a Virginia resident upon request from an authorized Partner business system.
- A secure Health Level Seven (HL7) service that pushes laboratory testing results as processed to an authorized Partner business system.
- A secure service that nightly transmits each newly eligible Medicaid recipient to the authorized Partner claims processing system. Each record is formatted using an Accredited Standards Committee X12 (X12) transaction format.
- A batch service that nightly dumps all newly eligible Medicaid recipients from the enrollment system into a fixed-format export file. The export file is then securely transferred to a reporting system and loaded overnight.

## **Preface to Appendices**

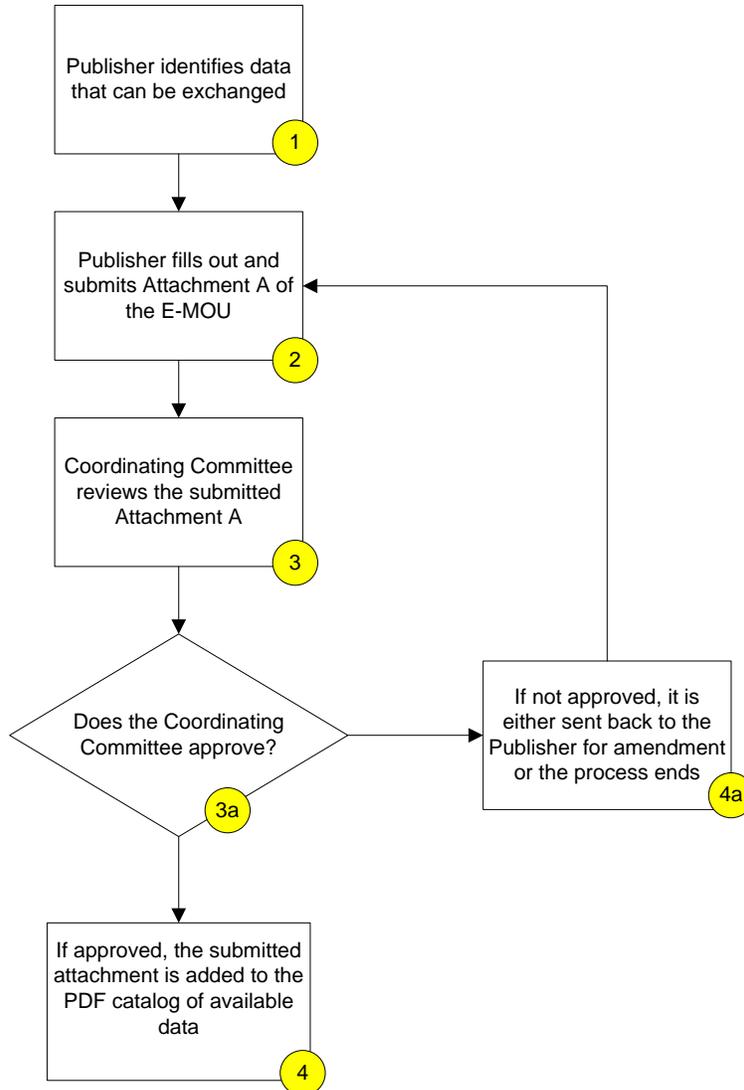
- A service that runs every time a new birth certificate is generated by Vital Records. The service extracts an image of the birth certificate and transfers the image file to the Vital Records document management system where it is uploaded.

Each Data Exchange Service must identify details specifying the business need, data content, security expectations, availability and dependency requirements. Those requirements are outlined in Appendix 1. In addition, each Data Exchange Service must be validated according to testing requirements as identified in Appendix 2 of this E-MOU.

# Appendix 1      New Publisher Requirements

## New Publisher Requirements

The workflow below illustrates the process of validating a Publisher Applicant. Detailed steps follow which further describe the process flow.



- Step 1. Applicant (Publisher) identifies what Data is available to be exchanged.
- Step 2. Applicant (Publisher) informs the Coordinating Committee which Data Service(s) they wish to exchange. Notification to the Coordinating Committee should be done in writing and delivered to the Coordinating Committee Recorder for distribution as appropriate. A template to collect these requirements can be found in Attachment A: Publisher Requirements Template for Data Exchange Services.
- Step 3. Coordinating Committee will review the Applicant (Publisher) request within ten (10) business days. The Coordinating Committee review will focus on the

## **Appendix 1      New Publisher Requirements**

authority of the Applicant to publish the Data and potential security, confidentiality or conflict of interest concerns.

- Step 4. If no concerns are identified, the Applicant is approved for membership as a Partner.
- Step 4a. If concerns are identified, the initial request will be returned to the Applicant (Publisher) by the Recorder for further clarification and possible amendment.

### **Attachment A: Publisher Requirements Template for Data Exchange Services**

The Publisher fills out the following fields on Attachment A and submits it via the E-MOU website for Coordinating Committee review:

#### **A. Publisher Information**

This section serves to provide basic information about the Publisher. Provide the name of the organization publishing the data, the name of the person submitting the form, and the name of the data service.

A description of Data Service should state the business purpose in terms that existing Partners, the Coordinating Committee and potential Partners, will understand. Be sure to identify value or benefits that a Partner may realize using this service. Also include risks and operational impacts incurred by not implementing service.

#### **B. Business Data of the Service**

Define the data fields included in the interface for this Data Service. Detail should be kept at the business level with technical specifics coming through implementation guides or documents. In addition to the name of each field in the data, additional attributes are defined to fully describe each element including:

- i. Data type - defines the form of Data included so the consumer of the service better understands possible values for that type; the operations that can be done on values of that type; the meaning of the Data; and the way values of that type can be reported. Valid types of business Data include:
  - Number – any numeric value
  - Money – special subset of Number to represent a financial transaction value
  - Boolean – denotes positive or negative value; can be interpreted as Yes/No; True/False; 0/1
  - String – defines the value as an alphanumeric string; variable length
- ii. Source of the Data – identifies where the Data originated from, useful in understanding how to interpret the data values, how to protect the Data and how the Data can be operated on. Typical sources include:

## **Appendix 1      New Publisher Requirements**

- Citizen –was provided by a Citizen or User
  - Partner – sourced from any participating organization that is a signatory to this E-MOU, either active or inactive with the Exchange
  - 3<sup>rd</sup> party –is provided by an external third party entity, not affiliated with any Commonwealth Organization
  - SSA – field content came from the Social Security Administration
  - IRS – field content came from the Internal Revenue Service
  - DHS - field content came from the Department of Homeland Security
  - CMS - field content came from the Centers for Medicare and Medicaid Services
  - Other
- iii. Origin – further defines the source of the Data including the system, application and data field which were the source of the content. Serves to clarify the applicable business functions allowed with the data content.
- iv. Special format assumptions – identifies special formatting that should be applied to the field content by the Partner consuming the service. Formatting is based on patterns which can be used to define input/output masks on the field. Example patterns include:
- (###) – field value must be numeric up to 999.
  - (###.##) – field value must be numeric up to 999 and allows 2 digits of decimal precision
  - (0) – field value must be between 0 and 9; zero will be treated as a default
  - (\$#.00) – field value must be up to \$99.99; fractional parts of a dollar will preserve ten and one digits by retaining a zero.
  - (MM/DD/YYYY) – field value will be treated as a multi-part date field
  - (APPROVED|REJECTED|PENDED) – field value must be one of the pre-defined values listed
- v. Security Requirements –additional security considerations should be applied to this data field within data. Recognized types include:
- PII – Protected Personally Identifiable Information
  - PHI – Treat as Protected Health Information
  - MH/BH – Treat as mental/behavioral health data
  - PCI – Payment Card Industry
  - SSA – Treat as SSN content under Virginia legislation
  - EDUCATION – Treat as educational data, subject to FERPA (Family Educational Rights and Privacy Act)
  - SUBSTANCE ABUSE – Treat as substance abuse information under federal law

### **C. Delivery Model**

This section serves to define the business requirements that trigger the interface for this service.

## **Appendix 1      New Publisher Requirements**

### **D. Physical Designation of the Service**

This section serves to outline details about the physical implementation of the data service. As previously noted, most of the technical details on data services will be found in related IT documents such as the Commonwealth SOA Governance Plan, CMS Interconnection Security Agreement and Partner-specific technical implementation standards.

In this section, identify where the physical description of the data service can be found. For Enterprise Service Bus-based shared services, it's expected that the MQ SOA Catalog will be the repository for shared services. For Partner-defined web-based services, the definition should be in a Partner-supplied archive. Such an archive will be accessible to Partners who potentially want to access the service, to enable design, development and testing.

Where possible, data services should comply with interface standards approved by the VITA Data Governance team. Identify which interface standard is being leveraged from the VITA inventory. If the data service does not follow a Data Governance approved standard, identify the business rationale for this approach.

If the data service requires additional logging or archiving capabilities beyond the baseline provided by the Data Exchange, outline the business requirements for these capabilities. Clarify if the additional requirements have impact on Data availability or security requirements.

### **E. Security Requirements**

Identify if the data service must comply with specific security requirements because it transmits protected content such as Protected Personally Identifiable Information or Protected Health Information. Identify the business requirement that mandates such protected information be transmitted. Reference Organization System Security Plans defined for the Commonwealth Security group as compliance material.

Evaluate if additional Partner-specific restrictions should be applied on the data service transmission. Include User or Group level restrictions if applicable. If the data is of a protected nature, it may be required to only share the content with a subset of specifically authorized Partners. Identify the business needs that define which Partners should have access to (or are prevented from accessing) the data service content. Business needs may include requirements stipulated by Applicable Law and/or functional requirements defined by Coordinating Committee Partners.

If the Data is protected and Citizen based in origin, it's likely that Citizen Authorization must be obtained before the content can be shared with Data Exchange Partners. Confirm that Applicable Law has been reviewed and if existing Data Exchange Authorization language

## **Appendix 1      New Publisher Requirements**

will allow Data Transmittal. If additional authorization is required, identify the legal requirements to be addressed and then state why it is necessary to share the Data.

### **F. Service Level Agreements**

Document what business timeframes the data service must be available to Partners. Relate availability to a stated business requirement. Is this a high-availability service that should be available 24x7 because citizens might access at any time? Is the data service only required during business hours such as when a call center will be open?

Identify if this data service mandates specific business continuity or disaster recovery requirements. Do these include specific expectations regarding Data loss during an event? What timeframe expectations exist if the data service must be recovered in a disaster? Link these points to a stated business requirement.

Document Operating Measures for the data service. Consider what the expected transaction load for the data service will be per 15 minutes while operating. Define if the data service will experience peak volume periods, per day, week, month or seasonally. If a real-time data service, define the expected response time in seconds during normal and stressed operation.

### **G. Related Service Dependencies**

Define any data services that must be executed in conjunction with this service. Identify the business nature of the workflow between these services. Capture the order dependency (sequence) the services must be executed under. Declare any special business assumptions that may exist because these services must work as a transaction.

### **H. On-boarding Validation Checklist**

Defined by the Publishing Partner, outlines the strategy to validate a new Subscribing Partner's successful integration and use of a data service. The On-boarding Validation Checklist should define the approach on how to on-board a Subscriber as a consumer of the service. This includes the testing objective, methods for testing new functions, total time, resources required, testing environment and any testing assumptions being made.

The test cases will exercise various integration aspects with the service including both normal operations and exception error handling from the client/consumer side of the service.

Each test case should include:

- i. Case # - a unique identifier for this test in the overall validation plan
- ii. Test Scenario – a description of the test script to be performed. Must define input testing values and any other environmental requirements to be used.

## **Appendix 1      New Publisher Requirements**

- iii. Test Type – defines the:
  - Positive – test case validates successful function or feature in the data service interface. Test results identify expected data that should be received using the service accurately.
  - Negative - test case validates exception handling with the data service. Test results identify the error condition to be expected.
  - Stress - test case serves to validate the data service and Partner interface can perform as expected in a high demand situation.
  - Endurance - test case serves to confirm the data service and Partner interfaces will perform positively during a sustained period of execution.
- iv. Expected Results – description of the expected results of the test case.

### **I. Pricing**

Enter the rate structure for the Data Exchange Service. Note whether the rate is different for public vs. private subscribers, as well as any options such as individual or flat rates. If this is an ad hoc exchange, explain that subscribers will need to contact you directly for pricing information. If the Data Exchange Service is provided at no-cost; leave blank.

### **J. Other Required Documents or Agreements**

Enter any other documents or agreements that will be required prior to onboarding, such as Business Associate Agreements, non-disclosure agreements, etc.

### **K. Required Transport Mechanism (Only applicable to ETL)**

Explain what transport protocol will be used: FTP, FTPS, PDP, NAS, etc. Keep in mind any security requirements for the protection of the data.

### **L. Physical Designation of the Service (Only applicable to ETL)**

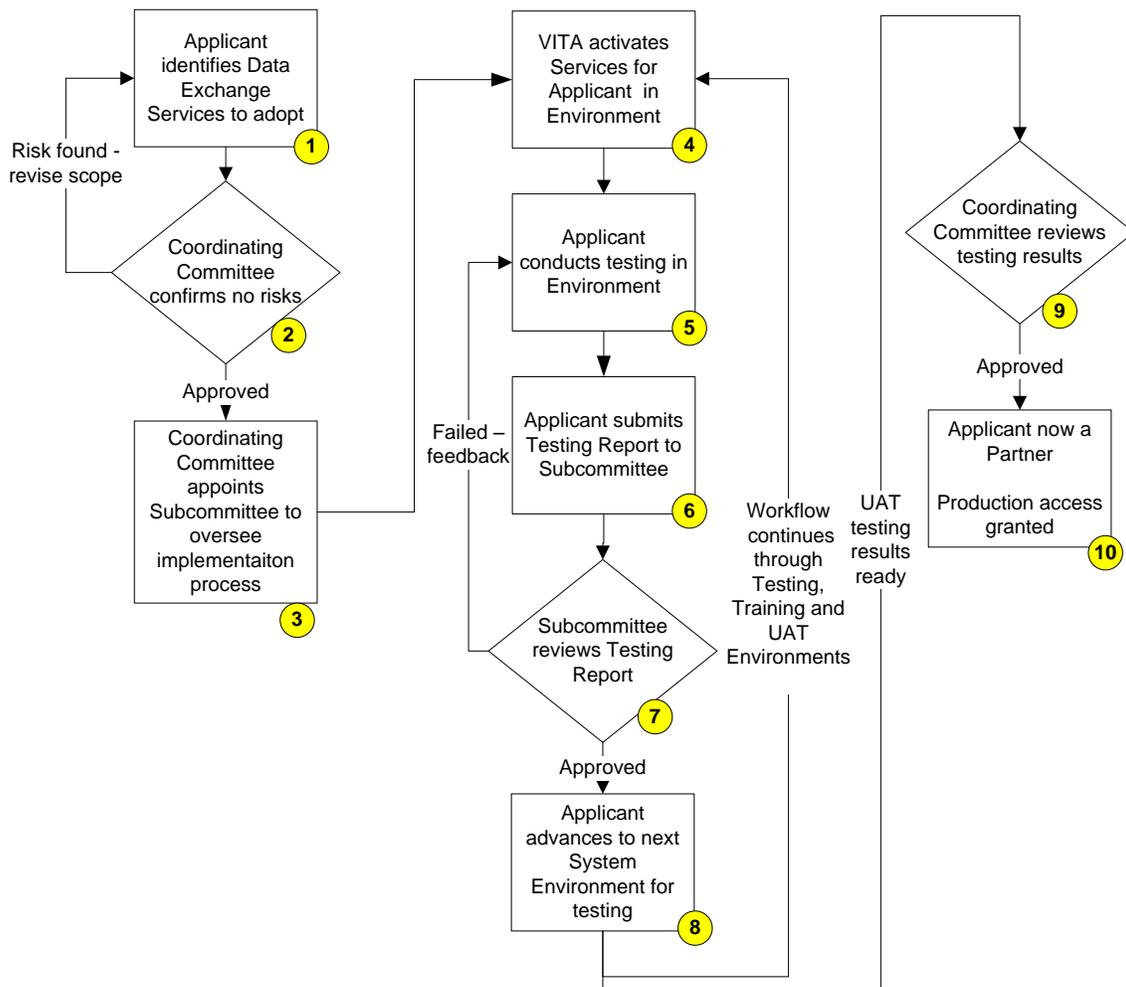
- Define the format of the file (XML, CSV, Fixed etc.).
- Document whether the file includes quality control header/footer rows. Provide content specifics for those rows, including any mandated requirements to retain header/footer rows for labeling, such as confidential etc.
- Define where the file layout is archived.
- Document whether the data service enforces special transaction logging requirements and define any requirements.
- Document whether the data service enforces additional transaction archiving requirements and define any requirements.

## Appendix 2      New Subscriber Requirements

### New Subscriber Requirements

This section describes the on-boarding activities to be performed by a potential new Partner to the Data Exchange or an existing Partner wishing to access new Data Exchange Services (referred to as Subscriber Applicant).

The workflow below illustrates the process of validating a Subscriber Applicant. Detailed steps follow which further describe the process flow



#### **A. Subscriber Selects Services to Adopt**

- Step 1. Applicant (Subscriber) informs the Coordinating Committee which Data Services they wish to access. Notification to the Coordinating Committee should be in writing and delivered to the Coordinating Committee Recorder for distribution as

## **Appendix 2      New Subscriber Requirements**

appropriate. Attachment B: Subscriber Requirements Template for Data Exchange services is to be used by Subscriber Applicants to request access to published services.

- Step 2. Coordinating Committee will review the Applicant (Subscriber) request within ten (10) business days. The Coordinating Committee review will focus on the authority of the Applicant to access the Data and potential security, confidentiality or conflict of interest concerns that might be raised if the Applicant has access to the data content available from the selected Data Service(s).
- If concerns are identified, the initial request will be returned to the Applicant (Subscriber) by the Recorder and they will be asked to clarify need and/or re-scope their request.
- Step 3. If no concerns are identified, the Applicant is approved to begin testing.
- Step 4. VITA will schedule and activate the selected Services for the Applicant in the Development environment within ten (10) business days.
- Step 5. Applicant may begin testing with the selected services in the Development environment.

### **B. Subscriber Conducts Tests**

- Testing can be conducted using the approved eHHR automated testing tools, or performed manually by the Applicant.
- Step 5. Testing will focus on peer-to-peer testing of the Applicant's system against an implementation of the selected Service(s) in the target environment.
- Validation is concerned with confirming that the interactions occur successfully as described by the selected Service(s) On-boarding Validation Checklist.
- Step 6. Testing will be accomplished by performing the test cases as identified in the selected Service(s) On-boarding Validation Checklist, and capturing the evidentiary artifacts defined in the On-boarding Validation Checklist to enable review by the Coordinating Committee

### **C. Subscriber Reports Test Results**

- Step 6. Although the Coordinating Committee expects to be in close contact with an Applicant during the testing process, the Applicant is required to submit a test report to the Coordinating Committee, accompanied by logs, screen shots, and other evidentiary artifacts as identified in the selected Service(s) On-boarding Validation Checklist.

### **D. Validation by Coordinating Committee**

- The Coordinating Committee will review the produced evidence, consulting with its Subcommittees as may be required.

## **Appendix 2      New Subscriber Requirements**

- Step 7. The Coordinating Committee will provide an opinion of the Applicant's test report within ten (10) business days from submission.
- Step 8. With approval from the Coordinating Committee, the Applicant may proceed to the next environment in the promotion sequence.
- If the Coordinating Committee does not approve the Applicant's test report, the Coordinating Committee will advise the Applicant with specific remediation guidance to improve compliance when re-testing (return to Step 5).
- The workflow is repeated by the Applicant for Development, Testing, Training and User Acceptance (UAT) environments. Each must be performed in sequence.
- Step 9. Once the Applicant has successfully completed UAT testing, the Applicant's test results will be reviewed by the Coordinating Committee for Production environment access.
- Step 10. If Coordinating Committee approves UAT test results, Production access is granted and the Applicant is approved as a Partner.

### **Attachment B: Subscriber Requirements Template for Data Exchange Services**

The Subscriber fills out the following fields on Attachment B and submits it via the E-MOU website for Coordinating Committee review:

#### **A. Subscriber Information**

Enter the following information:

- Subscriber name
- Subscriber type (public or private)
- Person's name filling out Attachment B
- Email address
- Phone number
- Mailing address
- Billing address (if different than mailing address)

#### **B. Data Service Information**

Answer the following questions:

- Define which published service you wish to subscribe to
- Describe how this data sharing will improve service delivery
- What date would you like to receive the data?
- What date will you stop receiving this data?
- Will the pricing be by individual record or flat rate?
- What rate will you be charged?

## **Appendix 3 Procedures for Suspending a Partner or Terminating a Partner**

### **Section 1: Suspension**

#### **A. Voluntarily by the Partner**

- 1. Service Level Interruptions.** Partners may experience temporary service level interruptions from time to time. These service level interruptions may be planned or unplanned. A service level interruption may result in a Partner having to temporarily cease Data Transmittals with other Partners. To ensure that all Partners are aware of service level interruptions, the Partner experiencing the service level interruption agrees to notify VITA, or the appropriate ITSP, of the interruption prior to the interruption, if planned, or as soon as reasonably practicable after the interruption begins, if unplanned. VITA, or the appropriate ITSP, shall simultaneously notify all other Partners and Members of the Coordinating Committee of the interruption. Since a service level interruption does not involve the suspension of a Partner's Digital Credentials, the Partner agrees to be responsible for taking all technical actions necessary to resolve a service level interruption. During a service level interruption, the Partner agrees to continue to comply with the terms and conditions of the E-MOU.
- 2. Voluntary Suspension.** If a Partner decides that it requires a temporary suspension of its Digital Credentials and its responsibility for complying with the terms of the E-MOU, it agrees to provide Notice to the Coordinating Committee Recorder of its need for a temporary voluntary suspension at least twenty-four (24) hours prior to commencing its voluntary suspension. The Notice shall specify the reason for, the commencement date of, and the duration of the voluntary suspension.

#### **B. With Cause by the Coordinating Committee**

Upon receipt by the Coordinating Committee Recorder of a complaint, i.e. a report or other information about a Partner questioning whether a Partner is creating an immediate threat of Data Breach or will cause irreparable harm to another Partner or a Citizen, the Coordinating Committee shall have the ability to investigate the complaint and determine whether such Partner should be suspended. The process for conduct of this investigation is outlined in section B.2 below.

When the complaint or evidence indicates that a suspension must be implemented immediately and, in the sole judgment of the Chairperson it is not practical to delay the suspension while process B.2 is conducted, process B.1 may be invoked by the Chairperson. The Coordinating Committee Chairperson shall constrain use of section B.1 to situations where:

## **Appendix 3 Procedures for Suspending a Partner or Terminating a Partner**

- i.) Evidence exists that a Partner is known to be breaching and is uncommunicative or is unwilling to voluntarily suspend such breaching activity pending an investigation; or
- ii.) Evidence exists that a Partner is suspected to be breaching and is uncommunicative or is unwilling to take immediate action to mitigate such breach threat activity pending an investigation.

If the Chairperson is unavailable or is affiliated with the complaint or evidence as either the complainant or the offender, the vice Chairperson shall act in the Chairperson's stead for all matters related to the complaint.

### **B.1 Urgent Partner Suspension for Cause *Preceding* Coordinating Committee Investigation**

The Chairperson shall immediately:

- Notify VITA, or the appropriate ITSP, and request that VITA, or the appropriate ITSP, take all technical actions necessary to carry out the suspension including, but not limited to, suspension of the Partner's Digital Credentials;
- Notify the suspended Partner of the suspension.
- Proceed with Process B.2

### **B.2 Coordinating Committee Investigation of Partner Activity having potential to lead to Partner Suspension for Cause**

The Chairperson shall immediately:

- Call a special meeting of the Coordinating Committee to inform the committee of the complaint having potential to lead to Partner suspension.
- Appoint a subcommittee to investigate the complaint.
- Direct the Coordinating Committee Recorder to immediately notify the Partner(s) in question of the investigation.

The Coordinating Committee's Investigation sub-committee shall meet as soon as practicable, but no later than five (5) business days after the receipt of the complaint by the Coordinating Committee, to evaluate the complaint. If suspension of a Partner has been effected by process B.1, the Coordinating Committee's Investigation sub-committee shall meet and begin their investigation work within two (2) business days of the urgent suspension. The Coordinating Committee's Investigation sub-committee shall consult with and report its progress and findings to the Coordinating Committee.

If the Coordinating Committee has not resolved the complaint within thirty (30) days after it was first referred to the Chairman (or such longer period as agreed to in writing by the Partners who are parties to the complaint), then the complaint shall be simultaneously

### **Appendix 3 Procedures for Suspending a Partner or Terminating a Partner**

escalated to the relevant Secretaries for resolution. If the Secretaries cannot agree on a resolution of the complaint, then the Secretaries may escalate the complaint and consult with the Governor's Chief of Staff for final resolution.

If, through the investigation, the Coordinating Committee determines that a Partner is (i) creating an immediate threat or (ii) will cause irreparable harm to another party including, but not limited to, another Partner, a User, VITA, or the appropriate ITSP, or an individual whose Data are exchanged pursuant to the E-MOU, the Coordinating Committee may suspend the Partner. Such suspension shall be tailored to address the threat posed by the Partner.

The Coordinating Committee Recorder shall immediately communicate the suspension to VITA, or the appropriate ITSP, and request that VITA, or the appropriate ITSP, take all technical actions necessary to carry out the suspension including, but not limited to, suspension of the Partner's Digital Credentials. As soon as reasonably practicable after suspending a Partner, but in no case longer than twelve (12) business hours, the Coordinating Committee Recorder shall provide the suspended Partner with a written summary of the reasons for the suspension and notify all other Partners of the suspension.

The suspended Partner agrees to provide the Coordinating Committee with a written plan of correction or an objection to the suspension within five (5) business days of being notified of the suspension.

The plan of correction shall describe the action that the Partner is taking to address, mitigate and remediate the issue(s) that caused the Coordinating Committee to determine that a suspension was appropriate and include a timeframe for such actions. Any objection shall specify the reason that the Partner feels the suspension is inappropriate

The Coordinating Committee shall within five (5) business days of receipt of either a Plan of Correction or an Objection from the Partner:

- i. Meet and review a suspended Partner's plan of correction or objection;
- ii. Determine whether to accept or reject the plan of correction or affirm the suspension; and
- iii. Communicate such decision to the suspended Partner.

If the Coordinating Committee rejects the plan of correction, it shall work in good faith with the suspended Partner to develop a mutually acceptable plan of correction. If the Coordinating Committee and the suspended Partner cannot reach agreement on the content of the plan of correction or on the reasons supporting the suspension itself, the Coordinating Committee may submit the Dispute through the Dispute Resolution Process or terminate the Partner in accordance with Section 3.

## **Appendix 3 Procedures for Suspending a Partner or Terminating a Partner**

Any suspensions imposed shall remain in effect until the Partner is reinstated or terminated in accordance with the E-MOU. A Partner shall be suspended by the Coordinating Committee before the Committee can proceed with termination of the Partner.

### **Section 2. Reinstatement**

#### **A. After Voluntary Suspension by a Partner**

The Partner's notification of a voluntary suspension shall state the commencement date and the duration of the suspension. The Partner may extend the duration of the voluntary suspension should it be necessary as determined by the Partner.

Either on the date indicated by the Partner in the suspension or extension request or at an earlier time if requested by the Partner, VITA, or the appropriate ITSP, shall take all technical actions necessary to reinstate the Partner's ability to participate in the Data Exchange including, but not limited to, the reinstatement of the Partner's Digital Credentials.

#### **B. After Suspension with Cause by the Coordinating Committee**

When a Partner's ability to participate in the Data Exchange has been suspended by the Coordinating Committee with cause, the Partner shall provide evidence to the Coordinating Committee of the Partner's fulfillment of the obligations of its plan of correction. The Coordinating Committee shall review such evidence at its next regularly scheduled meeting following receipt from the Partner.

If the Coordinating Committee is not satisfied that the Partner has met its obligations under its plan of correction, the Coordinating Committee Recorder shall inform the Partner of the deficiencies. The Partner will have the ability to submit additional evidence that addresses such deficiencies or the Partner may terminate its participation in the Data Exchange.

When the Coordinating Committee is satisfied that the evidence presented indicates that the Partner has fulfilled its obligations under the plan of correction, it shall so inform VITA, or the appropriate ITSP, and request that VITA, or the appropriate ITSP, take all technical actions necessary to reinstate the Partner's ability to participate in the Data Exchange including, but not limited to, the reinstatement of the Partner's Digital Credentials. The Coordinating Committee Recorder shall inform all other Partners of such reinstatement.

## **Appendix 3 Procedures for Suspending a Partner or Terminating a Partner**

### **Section 3. Termination**

#### **A. Voluntarily by the Partner**

All Notifications of termination by a Partner shall be directed to the Coordinating Committee Recorder in writing at least ten (10) business days prior to the termination date. Upon receipt of a Partner's Notification of voluntary termination, the Coordinating Committee Recorder shall promptly notify all other Partners of the termination. The Coordinating Committee Recorder shall request that VITA, or the appropriate ITSP, take all technical actions necessary to carry out the termination including, but not limited to, termination of the Partner's Digital Credentials.

#### **B. With Cause by the Coordinating Committee**

If, after further investigation following its suspension of a Partner for cause in accordance with Section 1 of this Appendix, the Coordinating Committee determines that there is a substantial likelihood that the Partner's acts or omissions create an immediate threat of Data Breach or will cause irreparable harm to another Partner or a Citizen, the Coordinating Committee may terminate the Partner.

If the Coordinating Committee finds that a Partner is in material default of the performance of a duty or obligation imposed on the Partner by the E-MOU, it shall notify the Partner, in writing, of such default. Material defaults include, but are not limited to, failure to comply with:

- any privacy, security or confidentiality obligations in the E-MOU;
- repeated failure to fulfill the duties of a Partner, including a requesting or responding Partner as provided for in the E-MOU; and
- any Breach of the representations in the E-MOU.

If the Partner does not substantially cure its material default within thirty (30) days following receipt of the written Notice of such default from the Coordinating Committee, the Coordinating Committee may terminate the Partner. During the cure period, the Coordinating Committee shall have the ability to continue any existing suspension in accordance with Section 1 of this Appendix.

The Coordinating Committee Recorder shall immediately communicate to VITA or the appropriate ITSP the decision to terminate a Partner and request that VITA, or the appropriate ITSP, take all technical actions necessary to carry out the termination including,

### **Appendix 3 Procedures for Suspending a Partner or Terminating a Partner**

but not limited to, termination of the Partner's Digital Credentials. The Coordinating Committee Recorder shall notify all other Partners of the termination.

## **Appendix 4 Process to Amend the eHHR Enhanced MOU**

### **Section 1. Retention and Dissemination of the E-MOU**

The official, executed version of the E-MOU shall be maintained in an electronic form and housed on the eHHR SharePoint E-MOU website. This site will be accessible to all E-MOU Partners including support staff and non-voting representatives.

### **Section 2. Submission of Proposed Amendments to the E-MOU**

Any Partner may submit in writing to the Coordinating Committee Recorder a request for an amendment to the E-MOU. All requests for proposed amendments shall identify:

- The section of the E-MOU that is the subject of the requested amendment (if any);
- A description of why the requested amendment is necessary;
- The proposed language for the requested amendment; and
- An analysis of the expected impact of the requested amendment.

### **Section 3. Consideration of Proposed Amendments to the E-MOU**

If, after considering the request, the Coordinating Committee determines that the request does not have merit, it shall communicate this determination to the requesting Partner.

If, after considering the request, the Coordinating Committee determines that the request has merit, the Coordinating Committee shall identify the timeframe to seek Partner approval of the recommended amendment.

When the Coordinating Committee informs the Partners of its recommendation for amendments to the E-MOU and seeks Partner approval of such amendments, the Coordinating Committee Recorder shall provide Partners with the following information:

- A copy of the proposed amendment to the E-MOU;
- Description of why the requested amendment is necessary and any foreseeable impact of the amendment;
- Statement regarding whether the proposed amendment is necessary in order for the Coordinating Committee or Partners to comply with Applicable Law; and
- Projected effective date for the proposed amendment.

### **Section 4. Approval or Rejection of Proposed Amendments to the E-MOU**

The Coordinating Committee shall meet to vote on recommending proposed amendments to the E-MOU. For proposed amendments to be recommended by the Coordinating Committee, at least two-thirds of the Members of the Coordinating Committee must approve the amendment.

## **Appendix 4      Process to Amend the eHHR Enhanced MOU**

Once an amendment is recommended by the Coordinating Committee, all Partners are advised to sign the amendment to the E-MOU prior to the effective date of the amendment or terminate their participation in accordance with Appendix 3 of the E-MOU.

## **Appendix 5      Change Process for Data Exchange Services**

### **Section 1.      Requests for Change**

#### **A. Development Changes**

The Coordinating Committee shall have the authority to adopt new E-MOU Performance and Service Specifications and use of Emergent Specifications, and to adopt amendments to, or repeal and replace, the E-MOU Performance and Service Specifications (collectively a “Development Change”). Specifications for Services must conform to those found in Appendix 1 of this E-MOU.

#### **B. Compliance Changes**

The Coordinating Committee shall have the authority to adopt new or to make Changes to existing E-MOU Performance and Service Specifications that are necessary for: (1) compliance with Applicable Law; or, (2) to maintain the integrity of Data being exchanged (collectively a “Compliance Change”). For Compliance Changes, and upon request from the Coordinating Committee, a task group may evaluate the Change and provide comments to the Coordinating Committee.

### **Section 2.      Receipt**

All Requests for Changes shall be directed in writing to the Coordinating Committee Recorder via the Data Exchange website. The Coordinating Committee Recorder shall catalog all Requests for Changes upon receipt.

The catalog shall include:

- i. Type of the proposed change (e.g. new, amendment, repeal)
- ii. Name and version number of the specification;
- iii. Whether the proposed change is a Development Change, Compliance Change or a Request for Consultation;
- iv. Brief description of the reasons for the proposed change (e.g., to enhance metadata available about a document, to meet requirements of a new use case or to comply with a specific law or regulation);
- v. Description of the actual changes;
- vi. Preliminary analysis of the potential business and technical impact to Partners and their Users; and
- vii. Copy of the specification.

The catalog will be made available on the Data Exchange website.

### **Section 3.      Evaluation**

## **Appendix 5      Change Process for Data Exchange Services**

The Coordinating Committee shall, within five (5) business days after being informed by the Recorder of receipt, forward the Request for Change to a task group designated by the Coordinating Committee for technical evaluation of the request and to make a recommendation for action to the Coordinating Committee. During consideration of the Request for Change, the task group may request additional information from the Coordinating Committee, Partners, or the requesting Partner, as the task group deems reasonably necessary.

### **A. Evaluation Criteria for Proposed Changes**

1. **Evaluation of Development Changes.** If the change is a Development Change, the Coordinating Committee Recorder shall ensure each Partner is provided a copy of the original proposed Change. Each Partner shall respond in writing to the Coordinating Committee Recorder by a designated response date with the following information:
  - i. Will implementation of the Development Change have a significant adverse operational or financial impact on the Partner;
  - ii. Will implementation of the Development Change require the Partner to materially modify its existing agreements with its Users or third parties;
  - iii. Does the Partner believe that implementation of the Development Change will require an amendment to the E-MOU, including amendments to the Permitted Purposes; and
  - iv. For a Development Change designated as optional, will the Partner decline to implement the change?

The Partner agrees to provide supporting reasons or rationale for each response where the Partner responds in the affirmative. The task group or the Coordinating Committee may request additional information from Partners to further evaluate the responses.

2. **Determination of Development Changes.** The task group shall review responses from the Partners to inform its recommendation to the Coordinating Committee about the proposed change. The criteria when considering the proposed change shall include:
  - i. If the change has a significant adverse operational or financial impact on at least 20% of Partners;
  - ii. Does the change require at least 20% of Partners to modify their existing agreements with Users or third parties; or
  - iii. Require an amendment to the E-MOU.

In addition, the task group shall consider the implications of the change to the policies and procedures for the Data Exchange.

## **Appendix 5      Change Process for Data Exchange Services**

If a new Organization becomes a Partner after Partners have been asked to respond to questions about the Development Change but before the designated response date, this new Partner will be given an opportunity to respond by the designated response date.

The task group shall present its recommendation to the Coordinating Committee at the Coordinating Committee's next regularly scheduled meeting following the designated response date. The Coordinating Committee shall review the task group's recommendation and make a final recommendation regarding whether the Development Change is an Approved change.

3. **Evaluation of Compliance Changes.** If the Change is a Compliance Change, the task group shall review the Change to assess its impact. The task group shall meet with the Coordinating Committee and present its findings and recommendations on the Compliance Change within three (3) weeks of the task group receiving the Compliance Change. The Coordinating Committee shall review the task group's recommendation and make a final recommendation to all Partners within two (2) weeks of receiving the task group's recommendation.
4. **Evaluation of the Timeline for Implementation of the Change.** For both Development Changes and Compliance Changes, the task group shall assess and make recommendations to the Coordinating Committee on the timeline for implementing the Change including, but not limited to, the number of prior versions of the Specification that should be supported and the amount of time that Partners should be given to migrate to the new Specification. The task group shall consider:
  - i. Whether the Change impacts interoperability among the Partners;
  - ii. The number of versions of the Specification that will be supported for backward compatibility purposes and the business implications of such support;
  - iii. If multiple versions will be supported, a sunset date for such support as the multiple versions are collapsed;
  - iv. The business implications for Partners related to migrating to the new Specification;
  - v. The number of Partners and number of transactions that will be impacted by the new Specification;
  - vi. The amount of time that Partners should be given to migrate to the new Specification; and
  - vii. Sunset dates as "old" specifications are retired.

The task group shall present its recommendations regarding implementation to the Coordinating Committee at the same time it presents its other recommendations regarding the same Change to the Coordinating Committee. The Coordinating Committee shall review the task group's recommendation and make a final determination regarding the timeline.

## **Appendix 6 Procedures for Breach Notification**

### **Section 1. Procedures for Partner Breach Notification**

#### **A. Notification Process**

1. Upon initial indication of a Breach, the Partner(s) responsible for or affected by the Breach shall report to the Commonwealth's Chief Information Officer in accordance with Applicable Law and state policy. Such reports shall be made to the Chief Information Officer within 24 hours from when the Partner discovered or should have discovered the occurrence. Partners shall also comply with any Applicable Law regarding Breaches, including Virginia Code § 18.2-186.6 and Virginia Code § 32.1-127.1:05, if applicable.
2. Following Notification to the Commonwealth's CIO, the Partner(s) shall immediately upload the Notification regarding the Breach to the secure portion of the Data Exchange website to which only Members of the Coordinating Committee have access and send an email to the Coordinating Committee Recorder notifying the Committee that the Notification has been uploaded.

A secure section of the Data Exchange website shall be created solely for the purpose of Breach reporting. This website function shall be designed to automatically email all Coordinating Committee Members that a Breach Notification has been uploaded.

#### **B. Notification Content**

The Notification shall include sufficient information for the Coordinating Committee to understand the nature of the Breach. For instance, such Notification shall include, to the extent available at the time of the notification, the following information:

- One or two sentence description of the Breach;
- Description of the roles of the people involved in the Breach (e.g., employees, Users, Citizens, service providers, unauthorized persons, etc.);
- Type of Data Breached;
- Partners likely impacted by Breach;
- Number of Users or records impacted/estimated to be impacted by the Breach;
- Actions taken by the Partner to mitigate the Breach;
- Current Status of the Breach (under investigation or resolved); and the
- Corrective action taken and steps planned to be taken to prevent a similar Breach.

The notification shall not include any Confidential or Protected Data. The Partner agrees to supplement the information contained in the Notification as it becomes available. Supplemental information should be uploaded to the secure portion of the Data Exchange website and directed to the same addresses used for the original Notification.

## **Appendix 6      Procedures for Breach Notification**

If, on the basis of the information available to the Partner, the Partner believes that it should temporarily cease Data Transmittals with all other Partners, it may undergo a service level interruption or voluntary suspension in accordance with Appendix 3 of the E-MOU.

### **Section 2.      Disposition of Breach Alerts and Notifications**

#### **A. Review of the Breach by the Coordinating Committee**

The Coordinating Committee Chairman shall facilitate a meeting of the Coordinating Committee upon receipt of the Breach alert or Notification for the purpose of reviewing the Notification and determining the following:

- i. The impact of the Breach or potential Breach on the privacy, security, confidentiality and integrity of the Data Transmittals;
- ii. Whether the Coordinating Committee needs to take any action to suspend the Partner(s) involved in the Breach or potential Breach in accordance with Appendix 3 of the E-MOU;
- iii. Whether the Coordinating Committee should take any other measures in response to the Notification or alert.
- iv. The Coordinating Committee shall, if needed, request additional information from the Partner(s) involved in the Breach or potential Breach to fulfill its responsibilities. However, with respect to potential Breach alerts, the Coordinating Committee is encouraged to hold inquiries and requests for additional information to allow the Partner time to determine whether a Breach actually occurred. After determination of a Breach (whether real or it is determined it is not a Breach), there should be documentation kept by the Partner of the event that occurred, in order to maintain records of review, in case of audit, etc.

#### **B. Voluntary Suspension or Termination by the Partner**

If, on the basis of the Breach alert or Notification, a Partner desires to cease Data Transmittals with Partner(s) involved in the potential or actual Breach, pursuant to Appendix 3 of the E-MOU, such Partner shall notify the Coordinating Committee Recorder of such cessation. The Coordinating Committee Recorder shall notify Members of the Coordinating Committee of each cessation Notification and keep a log of all such cessations for the Coordinating Committee's review.

#### **C. Determination of Breach Resolution**

Once complete information about the Breach becomes available, the Coordinating Committee shall meet to determine whether the actions taken by the Partner(s) involved in

## **Appendix 6      Procedures for Breach Notification**

the Breach are sufficient to mitigate the Breach and prevent a similar Breach from occurring in the future. Once the Coordinating Committee is satisfied that the Partner(s) have taken all appropriate measures, the Coordinating Committee shall deem the Breach resolved.

- i. This resolution will be communicated to all Partner(s) involved in the Breach and those Partners that ceased Data Transmittals with the Partner(s) involved in the Breach.
- ii. If those Partners do not resume Data Transmittals with the Partner(s) involved in the Breach, the Partner(s) involved in the Breach and cessation shall engage in the Dispute Resolution Process in accordance with this E-MOU.
- iii. Lessons learned on the root cause of the Breach will be communicated to all Partner(s), including those not involved in the Breach, to prevent a recurrence of the event in the future.

**Attachment A**  
**Publisher Requirements Template for Data Exchange Services**

**A. Publisher Information**

A.1. Enter Publisher Name

A.2. Enter Name of Person Submitting the Form

A.3. Data Service Name

A.4. Data Service Description

## Attachment A

### Publisher Requirements Template for Data Exchange Services

#### B. Business Data of the Service

##### B.1. Technical Specifications

*If this is a defined service with technical specifications, please reference the document and version number here. Regardless please fill out the table below.*

##### B.2. Data Fields

<b><u>Business Field Name</u></b>	<b><u>Group / Category</u></b>	<b><u>Data Type</u></b>	<b><u>Business Source</u></b>	<b><u>Origin</u></b>	<b><u>Special Format</u></b>	<b><u>Security Requirements</u></b>
<i>Field names in business friendly terms</i>	<i>Collection or organization of like data</i>	<i>number, money, Boolean, string</i>	<i>Citizen, Partner, 3<sup>rd</sup> party, SSA, IRS, DHS, CMS, etc.</i>	<i>Define where the data content came from? System/ Entity/ Field</i>	<i>Define as a mask to filter input/output</i>	<i>PII, PHI, PCI, SSA, etc.</i>

#### C. Delivery Model

*Short paragraph that defines the business requirements that trigger the interface for the service*

**Attachment A**  
**Publisher Requirements Template for Data Exchange Services**

**D. Physical Designation of the Service**

D.1. Where can the physical description be found?

*Define where in the SOA catalog this service can be found or other archive location.*

D.2. Does this Data Service align with a current VITA Data Governance approved interface?

*Define which standard aligned with or define why the service is not aligned.*

D.3. What format is the physical interface defined with?

*Define - MQ, WSDL, other based*

D.4. Logging Requirements

*Does the data service enforce special logging requirements? IRS, SSA, COV, etc.*

D.5. Archiving Requirements

*Does the data service enforce additional transaction archiving requirements?*

**Attachment A**  
**Publisher Requirements Template for Data Exchange Services**

**E. Security Requirements**

E.1. Does this interface require specific security requirements?

*Is there specific federal, state, or other language that empowers data sharing?*

E.2. Will the interface require additional citizen consent?

*If so – cite the Federal/State code that mandates consent be collected*

E. 3. Limit Subscriber Set

*Is the set of allowed Subscribing Partners limited? If so, enter it here.  
If not limited, leave blank.*

**F. Service Level Agreements**

F.1. Availability of service

*Define hours the service is required; 24x7, 8-5 business hours, weekends, etc.*

F.2. BC/DR requirements

*Does the service require additional business recovery or disaster recovery considerations? Indicate yes/no and if so, state the business need/requirement, along with any Federal/State code that mandates such.*

F.3. Transaction load/volume capacity expectations

*What's the expected transaction load per 15 minutes? What's the highest (peak) # of transactions expected in a business day?*

**Attachment A**  
**Publisher Requirements Template for Data Exchange Services**

F.4. Performance/response time expectations

*Is this a real-time service? Other? What's the expected response time in seconds?*

**G. Related Service Dependencies**

G.1. Define any Services that must be used in conjunction with this Service

<b>Name of related service</b>	<b>Define the relation to this service</b>
<i>Name of related service</i>	<i>Is it essential/compulsory as a required predecessor or invoked as a sub-service?</i>

G.2. Define special business assumptions that may exist because of these dependences

*Does this create additional requirements for security, data accuracy, reporting, etc? If so, state those additional requirements, including any mandated citations.*

**Attachment A**  
**Publisher Requirements Template for Data Exchange Services**

**H. On-boarding Validation Checklist**

H.1. Test Strategy

*Short paragraph defining the overall testing approach for Partners accessing this service*

H.2. Test Scenarios

<b>Case #</b>	<b>Scenario</b>	<b>Type of Test</b>	<b>Expected Result</b>
<i>1 to N</i>	<i>Describe the test case including input data values</i>	<i>Positive, Negative, Stress, Endurance</i>	<i>Describe the expected results</i>

**I. Pricing**

*Enter the rate structure for the Data Exchange Service. Note whether the rate is different for public vs. private subscribers, as well as any options such as individual or flat rates. If this is an ad hoc exchange, explain that subscribers will need to contact you directly for pricing information. If the Data Exchange Service is being provided at no-cost; leave blank.*

**J. Other Required Documents or Agreements**

*Enter any other documents or agreements that will be required prior to onboarding, such as Business Associate Agreements, non-disclosure agreements etc.*

**Attachment A**  
**Publisher Requirements Template for Data Exchange Services**

**K. Required Transport Mechanism (Only Applicable to ETL)**

*What transport protocol will be used, FTP, FTPS, PDP, NAS, etc. (keep in mind any security requirements for the protection of the data content)*

**L. Physical Designation of the Service (Only Applicable to ETL)**

L.1. What format is the file?

*Define the type of file being exchanged, XML, CSV, Fixed.*

L.2. Does the file include a header and/or footer row?

*Document if the file includes quality control header/footer rows. Provide content specifics for these rows, including any mandated requirements to retain header/footer rows for labeling, such as confidential, etc.*

L.3. Where can the physical description be found?

*Define where the file layout is archived.*

L.4. Logging Requirements

*Does the data service enforce special transaction logging requirements? If so, define those requirements.*

L.5. Archiving Requirements

*Does the data service enforce additional transaction archiving requirements? If so, define those requirements.*

**Attachment B**  
**Subscriber Requirements Template for Data Exchange Services**

**A. Subscriber Information**

A.1. Enter Subscriber Name

*Enter the name of the Subscribing Partner.*

A.2. Enter Subscriber Type (Public or Private)

*COV agencies are Public; all others are Private*

A.3. Enter Name of Person Submitting the Form

*Contact person at the Subscribing Partner*

A.4. Enter Email ID

*Contact e-mail address at the Subscribing Partner*

A.5. Enter Phone Number

*Contact phone number at the Subscribing Partner*

A.6. Enter Mailing Address

*Contact postal address at the Subscribing Partner*

A.7. Enter Billing Address

*Leave blank if the billing address is the same as the mailing address*

**Attachment B**  
**Subscriber Requirements Template for Data Exchange Services**

**B. Data Service Information**

B.1. Enter the Name of the Published Service

*Define which published service you wish to subscribe to*

B.2. Enter the Business Use

*Describe how this data sharing will improve service delivery*

B.3. Enter the Preferred Start Date

*What date would you like to start receiving the data?*

B.4. Enter the End Date

*What date will you like to stop receiving this data?*

B.5. Enter Pricing Type

*Will the pricing be by individual record or flat rate?  
Leave blank if the Data Exchange Service is being provided at no-cost.*

B.6. Enter Pricing Rate

*What rate will you be charged?  
Leave blank if the Data Exchange Service is being provided at no-cost.*