# State of Illinois
# Enterprise Memorandum
# Of Understanding (E-MOU)

# List of Appendices and Attachments

# HHS Enterprise Memorandum of Understanding (E-MOU)

WHEREAS, thirteen State agencies and multiple boards, commissions, authorities and tribunals of State government (the "Partners" or "Original Partners") currently have responsibility for the administration of the State's healthcare and human services programs and are members of the Illinois Health and Human Services Leadership Transformation Committee: these thirteen State agencies are the Department of Human Services, the Department of Aging, the Department of Healthcare and Family Services, the Department of Commerce and Economic Development, the Department of Employment Security, the Department of Public Health, the Department of Children and Family Services, the Department of Corrections, the Department of Juvenile Justice, the Department of Veterans Affairs, the Department of Central Management Services (for technology services), the Department of Innovation and Technology, and the Illinois State Board of Education;

WHEREAS, the Partners desire to securely exchange data as permitted or required by applicable law in order to increase the efficiency and effectiveness of programs they operate for the benefit of the citizens of the State of Illinois;

WHEREAS, this Enterprise Memorandum of Understanding ("E-MOU") does not preempt or contradict in any manner any statutory duties or authority required of or granted to, respectively, Partners; rather, the Partners enter into this E-MOU to enable their participation in the Data Exchange Service, as defined and set forth below;

WHEREAS, once the Partners enter into this E-MOU, they hope that other governmental entities desire to participate in the Data Exchange Service in the future, and each new entity shall be known as a "Partner";

NOW, THEREFORE, for and in consideration of the mutual covenants contained herein, the Partners mutually agree to the provisions set forth in this E-MOU.

## ARTICLE I
## INTRODUCTION

The purpose of this E-MOU is to allow for interoperability of data between the Partners. Interoperability is a national effort of technology and programmatic coordination. Interoperability refers to the ability of two or more systems or components to exchange information and to use the information for the benefit of the State and its clients.

## ARTICLE II
## DEFINITIONS

For the purposes of this E-MOU, the following terms shall have the meaning ascribed to them below.

a. **Applicable Law** shall mean all applicable federal and state laws and regulations.

b. **Authorization** shall have the meaning and include the requirements set forth at 45 CFR §164.508 and any similar Applicable Laws with additional requirements. Authorization shall be confirmed by execution of the Uniform Authorization to Exchange Information form or some other written authorization that meets the requirements of Applicable Law that applies to the Partner providing the data.

c. **Breach** shall mean all known incidents that result in the unauthorized access, use, or disclosure of data protected by federal or state laws.

d. **Changes** shall mean Developmental Changes (as used in Appendix 3 and defined in Appendix 3, Section 1.A) and Compliance Changes (as used in Appendix 4 and defined in Appendix 3, Section 1.B). Changes shall be managed in accordance with Appendix 3 of this E-MOU.

e. **Data** shall mean any information about an Individual, including but not limited to information that can be used to distinguish one person from another person and/or that is confidential under Applicable Law, and disclosed by one Partner to another Partner under this Agreement.

f. **Data Exchange Service** shall mean hardware, software programs, protocols, etc. that serves to securely and safely share Data between Partners. Requirements for Data Exchange Services are defined in Appendix 5 of this E-MOU.

g. **Data Request** shall mean a request for Data made by one Partner to another and defined by an approved E-MOU Specification.

h. **Data Transmittal** shall mean an electronic exchange of Data between Partners using agreed upon Specifications.

i. **Digital Credentials** shall mean a mechanism, such as a public-key infrastructure, that enables Partners to electronically prove their identity and their authority to conduct data transmittal with other Partners.

j. **Discloser** shall mean a Partner that discloses Data to another Partner through a transmittal in any format.

k. **Dispute or Disputed Matter** shall mean any controversy, dispute, or disagreement arising out of or relating to this E-MOU.

l. **Effective Date** shall mean the date of execution of this E-MOU by two or more Partners.

m. **Emergent Specifications** shall mean new technical specifications that existing and/or potential Partners are considering to implement to test the feasibility of the emerging technology, to identify whether the Specifications reflect an appropriate capability for the Partners, and assess whether the Specifications are sufficient to add as a production capability available to the Partners.

n. **Individual** shall mean a client or person whose data is maintained by a Partner and subject to exchange with participating agencies.

o. **Information Technology Service Provider or ITSP** shall mean a company or other organization that will support one or more Partners by providing them with operational, technical, cloud, or information technology services.

p. **Notice or Notification** shall mean a written communication sent to the appropriate Partner's representative in accordance with the other policies and procedures attached to this E-MOU.

q. **Operational Measures or Operational Data** shall mean information pertaining to the volume and performance of Data Transmittals pursuant to this E-MOU; such as activity counts, performance measures, uptime metrics, error rates, connection metrics and other indicators of activity. This aggregated data does not contain any individually identifiable data or protected content.

r. **Partner** shall mean any office, officer, including any statewide constitutional officer, division, or part thereof, including any agency, department, division, bureau, board, commission, authority or tribunal of State government, public building commission, and any combination of the above pursuant to an intergovernmental agreement which includes provisions for a governing body of the agency created by the agreement that is a signatory to this E-MOU, and any ITSP working specifically for the Partner.

s. **Partner Access and Disclosure Policies** shall mean those policies and procedures of a Partner that govern a User's ability to access, exchange, and transmit Data using the Partner's System, including privacy and security policies.

t. **Personally Identifiable Information (PII)** is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

u. **Production Data** shall mean Data created by a Partner in accordance with the Validation Plan and used by the Partner for Production purposes in a Production environment. Production data may contain PII or other data that is subject to State or Federal data protection requirements.

v. **Recipient** shall mean the Partner(s), users, vendors, and any other person or entity that receive(s) or has access to the Data through a Data Transmittal from a Discloser pursuant to this E-MOU.

w. **Specifications of Service or Service Specification or Specifications** shall mean the specifications established by Applicable Law or adopted by the Operational Committee that prescribe the Data content, technical, and security requirements needed to enable the Partners to Transmit Data. Specifications may include, but are not limited to, specific standards, services, and policies applicable to Data Transmittal pursuant to this E-MOU. The specification requirements are attached hereto as Appendix 5, and may be amended in accordance with Appendix 3 and 5.

x. **System** shall mean the software, portal, platform, or other electronic medium controlled by a Partner through which the Partner conducts its Data Transmittal related activities. For purposes of this definition, it shall not matter whether the Partner controls the software, portal, platform, or medium through ownership, lease, license, or otherwise.

y. **Test Data** shall mean Data created by a Partner in accordance with the Validation Plan and used by the Partner for Testing purposes in a Testing environment. Test Data in a Test environment shall not contain Production Data, unless the data has been obfuscated to ensure there is no PII data present or agreed on by all E-MOU Partners. In the case of such exceptions, all production level data security protocols must be adhered to.

z. **Testing** shall mean the tests and demonstrations of a Partner's System and processes used for interoperable Data Transmittal to assess conformity with the Emergent Specifications, Specifications and Validation Plan.

aa. **Transmit, Transmittal or Transmitting** shall mean, in varying tenses, to send Data electronically using the Specifications.

bb. **User** shall mean any employee of a Partner or individual or entity who has been authorized to access the Data through the respective Partner's System in accordance with Applicable Law.

cc. **Validation Plan** shall mean the framework for Testing and demonstrations for Partner seeking to use a Data Exchange Service. The Validation Plan is attached hereto as part of Appendix 6, and must be in compliance with Appendix 3 and Appendix 5.

## ARTICLE III
## RESPONSIBILITIES OF THE OPERATIONAL COMMITTEE

The Operational Committee is an advisory group reporting to the Secretary of the Department of Innovation and Technology. It will support secure Data Transmittal and develop the Specifications, including Emergent Specifications, with which the Partners shall comply in Data Transmittal pursuant to this E-MOU. The Committee is comprised of one representative from each of the Original Partners and is chaired by the State's Chief Data Officer (representing the Department of Innovation and Technology). The Committee will elect a Vice-Chair and a Secretary; additionally, one member of the Operational Committee will be the Technical Chair, one member will be the Security Chair, and one person will be the Privacy Chair. A quorum is comprised of seven or more members who are present in-person, telephonically, or through video conference and the Operational Committee shall use a majority of the Members voting process. Operational Committee members may send a Proxy to attend and vote on Committee items in their absence. For a one-time Proxy request, the Committee Chair must be notified in writing by the eMOU Partner Agency's Chief Executive of their intention to send a Proxy, with the name and title of the Proxy, at least 24 hours in advance of a scheduled eMOU Operational Committee meeting. For a blanket Proxy request, in which a Proxy is named in the event an eMOU Committee Member is absent for any eMOU Committee meeting during a 12 month period, the Committee Chair must be notified in writing by the eMOU Partner Agency's Chief Executive of their intention to use a blanket Proxy, with the name and title of the Proxy and the start and end dates of the blanket Proxy request. A blanket Proxy request may not exceed 12 months. The Operational Committee shall schedule meetings on a monthly basis, or more frequently as necessary or at the call of the Secretary of the Department of Innovation and Technology or designee.

The Operational Committee will conduct, at the request of the Secretary of the Department of Innovation and Technology or designee, as an entire body or individual members working together, the following activities regarding specific Data Exchange Services:

a. Maintaining a list of all E-MOU Partners, their designated representative(s) and their preferred contact information where they can be reached, which shall be made accessible to all E-MOU Partners by posting on a website;

b. Receiving reports of Breaches, notifying Partners of Breaches, receiving confirmation from Partners when the security of their Systems have been restored after Breaches, and notifying Partners when all issues leading to a Breach have been resolved. Notification of a Breach to the Operational Committee does not relieve the Partner of its responsibilities under Applicable Law, including any required notifications that a Breach has occurred and any related notifications required due to a breach of any shared information;

c. Advising the Secretary of the Department of Innovation and Technology or designee when to issue a finding or suspend data exchanges based on a sanctioned Incident Response Handling Plan and in accordance with Appendix 4 of this E-MOU;

d. Advising the Secretary of the Department of Innovation and Technology or designee how to resolve Disputes between Partners in accordance with this E-MOU;

e. Managing the amendment of this E-MOU in accordance with Appendix 2 of this E-MOU;

f. Developing, evaluating, prioritizing, and adopting Specifications, including Emergent Specifications, changes to such Specifications, and the artifacts required by the Validation Plan in accordance with Appendix 5 and Appendix 6 of this E-MOU. Any Specifications developed shall be consistent with Applicable Law;

g. Maintaining a process for managing versions of the Specifications, including migration planning;

h. Evaluating requests for the introduction of Emergent Specifications into the production environment used by the Partners to perform a Data Transmittal;

i. Performing impartial review of Partners' compliance with the Specifications as defined in Appendix 5 of this E-MOU; and

j. Work with the original Discloser Agency to respond to Freedom of Information Act Requests, subpoenas, court orders or other third party requests related to the Data.

k. Fulfilling all other responsibilities delegated by the Secretary of the Department of Innovation and Technology or designee to the Operational Committee as set forth in this E-MOU.

l. Right to conduct an audit of the environment of any Partner-specific IT system that will be receiving data through this E-MOU.

m. Create and maintain a record of any disclosure of Data made to any other person or entity not already denoted in an Attachment A to Appendix 5. The record of disclosure shall

record the name of any additional person or entity receiving the Data, the legitimate and legal interest of the disclosure, and a description of the Data included in the disclosure.

## ARTICLE IV
## USE OF DATA

a. **Permitted Purpose.** Partners shall only Request and Transmit Data in accordance with Applicable Law, including 45 CFR §164.508(c). Partners shall enforce this rule with its users, employees, vendors and any other person or entity that receives, sends, or has access to Data pursuant to this E-MOU.

b. **Permitted Future Uses.** Recipients shall only retain and use Data in accordance with Applicable Law, the business purpose as defined in the Specification Sheet for Electronic Data Interchange (EDI) Service and/or Extract, Transform and Load (ETL) Service when applying for a Data Exchange Service as described in Attachment C to Appendix 5, the data sharing document executed between the Recipient and the Discloser, and the Recipient's record retention policies and procedures. Recipients shall not disclose Data to any outside entity or person, including subcontractors, without the written permission of the Discloser.

c. **Management Uses.** The Secretary of the Department of Innovation and Technology, or designee, may request operational measures from Partners regarding use of exchanged data, and Partners agree to provide requested measures in accordance with Applicable Law, for the purposes listed in Article VIII of this E-MOU, Expectations, Duties, and Responsibilities of the Partners.

d. **Authorization**. The Partner certifies that unless permitted or required to share data by Applicable Federal and/or State law, it has obtained a Uniform Authorization to Exchange Information which permits it to disclose Data for the Individual served by the Partner for whom an inquiry is made, pursuant to this E-MOU. If the Partner does not have a signed Uniform Authorization to Exchange Information, but has a previously-signed Authorization, the previous authorization may be sufficient until the Uniform Authorization to Exchange Information is signed. Such Authorization may be included as part of the Individual's application form or it may be a separate consent to release form which is kept in the Individual's file. In either case, the Individual must sign the Authorization, or where the Individual is a minor, the Individual's parent or legal guardian. If the Individual has a representative authorized to act on his or her behalf, the representative may sign the release.

e. **Tracking of Authorizations**. The Partners agrees to track the expiration and/or revocation of Authorizations in compliance with the requirements of 45 CFR §164.508, and specifically

1) 164.508(b) (2) Defective authorizations. An authorization is not valid if the document submitted has any of the following defects: (i) the expiration date has passed or the expiration event is known by the covered entity to have occurred; (ii) the authorization has not been filled out completely, with respect to a required element; (iii) the authorization is known by the covered entity to have been revoked; (iv) the authorization creates a compound authorization (164.508(b)(3)) or violates the prohibition on conditioning authorizations (164.508(b)(4)); (v) any materials information in an authorization is known by the covered entity to be false.

2) 164.508(b)(5) Revocations of authorizations. An Individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that information has been shared already or action has taken place already in reliance on the authorization..

## ARTICLE V
## SYSTEM ACCESS POLICIES

a. **Autonomy Principle.** Each Partner agrees to have Partner Access and Disclosure Policies. Each Partner acknowledges that Partner Access and Disclosure Policies may differ among them as a result of differing Applicable Law and business practices. Each Partner agrees to be responsible for encrypting data in transit using current industry standard algorithms agreed on by the parties involved before transmission occurs based on the application of its Partner Access and Disclosure Policies to the requested Data. Each Partner shall comply with Applicable Law, this E-MOU, and all applicable Specifications in Transmittal of Data.

b. **Authentication.** Each Partner agrees to employ an approved credentialing service (for example, "Entrust" is a service provider that would provide PKI (Public Key Infrastructure) credentialing services.) through which the Partner, or its designee, uses the Digital Credentials to verify the identity of each User prior to enabling such User to Transmit Data. The "approved credentialing service" must meet State, Federal, and Industry standards. It must also be commonly used, verifiable, and known to as being used in existing Data exchanges.

## ARTICLE VI
## ENTERPRISE SECURITY

a. **General.** Each Partner agrees to proceed according to requirements contained in (FISM) NIST SP800-39, Managing Information Risk. Furthermore, each Partner shall be responsible for maintaining a secure environment compliant with State policies, standards and guidelines, and other Applicable Law that supports the Transmission of Data in compliance with the Specifications. Partners shall follow the specifics contained in (FISM) NIST SP800-47, Security Guide for Interconnecting Information Technology Systems and shall use appropriate safeguards to prevent use or disclosure of Data other than as permitted by this E-MOU, the (FISM) NIST SP800-47, and Applicable Law, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Data. Appropriate safeguards shall be those required by Applicable Law related to Data security, specifically as contained in (FISM) NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Additional safeguards recommended and/or required by the Secretary of the Department of Innovation and Technology or designee or the State's Chief Information Security Officer will be met, including but not limited to encryption of Data in transit and at rest using current industry standard algorithms agreed on by the parties involved before transmission occurs. Each Partner agrees to, as appropriate under Applicable Law, have written privacy and security policies, including Access and Disclosure Policies, in place before the Partner's respective Effective Date for data exchange, meeting both FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, and (FISM) NIST SP800-60 Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories. To the extent permitted under Applicable Law, Partners shall comply with any Specifications that define expectations with respect to enterprise security.

b. **Malicious Software.** Each Partner agrees to employ security controls so that Data

Transmittal will not introduce any viruses, worms, unauthorized cookies, Trojans, malicious software, "malware," or other program, routine, subroutine, or Data designed to disrupt the proper operation of a System or any part thereof or any hardware or software used by a Partner in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a System or any part thereof or any hardware, software or Data used by a Partner in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. Partner agrees to meet the requirements contained in (FISM) NIST S P800-53, Security and Privacy Controls for Federal Information Systems and Organizations, (FISM) SP800-60, Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories, and FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems.

c. In accordance with Applicable Law, each Partner on its side of the exchange shall be responsible for procuring, and assuring that its Users have or have access to, all equipment and software necessary for it to fulfill its responsibilities under this E-MOU. Each Partner shall ensure that it is meeting the requirements set forth in (FISM) NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations and that all computers and electronic devices owned or leased by the Partner used to store, transmit, receive, and permits access are properly configured, including, but not limited to, the operating system, web server, and Internet connectivity. Each Partner shall comply with FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems. Partners shall ensure that System solutions that store, transmit, receive, and permits access are compliant with the Specifications and with the requirements contained in (FISM) NIST 800-60, Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories.

d. Each Partner shall, through its agents, employees, and independent contractors, have the ability to monitor and audit all access to and use of its System related to this E-MOU, for system administration, security, and other legitimate purposes. Each Partner shall develop auditing activities that meet the requirements in (FISM) NIST SP800-137, Information Security Continuous Monitoring (ISCM) and shall perform those auditing activities required by the Specifications.

e. **Security Standards for Transmission of Data**. Data should be encrypted to appropriate framework or regulation relevant to the policy, using current Industry standard algorithms agreed on by the parties involved. Electronic signatures should be used in transmissions to identify the source and destination.

f. **Exception Process**. A Partner which does not yet fully meet the requirements set forth above in Article VI may apply to the Operational Committee with a proposed plan to share data during the process of coming into full compliance with the stated requirements. The request will be assigned to the Security Chair, who, in partnership with the Office of the State's Chief Information Security Officer, will review the request and provide a recommendation to the full Operational Committee.

## ARTICLE VII
## SPECIFICATIONS

a. **General Compliance.** Each Partner shall comply with all of the Specifications under this E-MOU, and identified hereto as Appendix 5, unless compliance would be a violation of Applicable Law.

b. **Adoption of Specifications.** The Partners hereby acknowledge the role of the Operational Committee as the mechanism whereby the Partners can jointly advise the adoption of Service Specifications and Emergent Specifications, and that the Operational Committee, at the direction of the Secretary of the Department of Innovation and Technology, may recommend the adoption of amendments to, or repeal and replacement of, the Service Specifications at any time, as outlined in Appendix 3 and Appendix 5 of this E-MOU.

c. **Specification Amendment Process.** The Specifications shall be amended as set forth in Appendix 3 of this E-MOU.

## ARTICLE VIII
## EXPECTATIONS, DUTIES, AND RESPONSIBILITIES OF PARTNERS

a. **Minimum Requirements for Partners Regarding Data Requests.** All Partners that make Data Requests, or allow their respective Users to make Data Requests, shall have a collaborative relationship and shall respond to Data Requests when made to them by another Partner in the affirmative, unless specifically prohibited by Applicable Law. The eMOU Operational Committee shall submit all Data Requests to the General Counsel's Office of the Agency from which the requested Data originates. If the request cannot be fulfilled, the Partner's General Counsel's Office shall provide the legal authority on why the request cannot be complied with and how to overcome the prohibition. A Partner's General Counsel shall fulfill its duty to respond to Data Requests by either (i) providing written approval of the Data Request within ten (10) business days and the Data Exchange Service will proceed as outlined in Appendix 5, unless a request is made to the Operational Committee to extend the response time, or (ii) respond to the Data Request within ten (10) business days that the Data is not available or cannot be exchanged, with the Legal authority on why the request cannot be complied with and how to overcome the prohibition. If no response is received by the Operational Committee from the General Counsel's Office of the Agency from which the requested Data originates within ten (10) business days, the Data Request will be considered approved and the Data Request process will proceed as outlined in Appendix 5. Partners must be approved to request Data from the specified Data Exchange Service as defined in Appendix 5 and 6. However, if the Data Transmission to Partners is specifically prohibited by Applicable Law, Partners shall work to identify if any edits, deletions or additional protections can be made to comply with Applicable Law and allow Data to be provided to a Partner. Partners shall provide the Operational Committee with plans and procedures for ensuring Data shared between the Partners continues to be protected in accordance with such laws.

b. **Users and Information Technology Service Provider (ITSPs).** Each Partner shall require that all of its Users and ITSPs perform Data Transmittal only in accordance with the terms and conditions of this E-MOU and the applicable Specifications, including without limitation those governing the authorization, use, confidentiality, privacy, and security of Data.

c. **Specific Duties of a Partner When Transmitting Data**. Whenever a Partner

Transmits Data to another Partner or User, the Transmitting Partner shall do so in compliance with Applicable Law, this E-MOU, the applicable Partner Access and Disclosure Policies, and the applicable Specifications.

d. **Privacy and Security.**

1. **Applicability of Privacy and Security Regulations.** To maintain the privacy, confidentiality, and security of Data, and in determining Data security (including but not limited to where the Enterprise information shall be maintained and who has access to the Data), each Partner shall comply with Applicable Law, applicable Partner Access and Disclosure Policies, the Specifications, this enterprise standard and this E-MOU, and will meet all of the requirements set forth by the State's Chief Information Security Officer in conformity with (FISM) NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

2. **Safeguards.** Partners shall use reasonable and appropriate administrative, physical and technical safeguards as defined by the State's Chief Information Security Officer in conformity with (FISM) SP800-47, Security Guide for Interconnecting Information Technology Systems, and comply with the Specifications to protect Data and to prevent use or disclosure of Data other than as permitted by this E-MOU.

3. **Breach Notification.** Partners shall report to the Secretary of the Department of Innovation and Technology or designee all Breaches that threaten the security of the State's databases and Data communications resulting in exposure of Data protected by federal or state laws, or other incidents compromising the security of the State's information technology systems with the potential to cause major disruption to normal agency activities based on the sanctioned Incident Response Handling Plan and in accordance with Appendix 4 of this eMOU. Such reports shall be made to the Secretary of the Department of Innovation and Technology or designee within 24 hours from when the Partner discovered or should have discovered the occurrence. Partners shall also comply with any Applicable Law regarding data breaches.

4. **Conflict of Obligations**. This Article shall not be deemed to supersede a Partner's obligations (if any) under relevant security incident, breach notification or confidentiality provisions of Applicable Law or pursuant to the Statewide Incident Response Plan.

5. **Conflict of Compliance.** Compliance with this Article shall not relieve Partners of any other security incident or Breach reporting requirements under Applicable Law including, but not limited to, those related to Individuals.

e. **Responsibilities of the Partners.** Each Partner hereby agrees to the following:

1. **Data Requested by the Operational Committee.** Except to the extent prohibited by Applicable Law, each Partner has provided, and agrees to continue to provide, the Operational Committee with all Operational Measures reasonably requested by the Operational Committee and needed by the Operational Committee to discharge its duties under this E-MOU or Applicable Law. Any Operational Measures provided by a Partner to the Operational Committee shall be responsive and accurate. Each Partner agrees to provide Notice to the Operational Committee if any Operational Measures provided by the Partner to the Operational Committee materially changes. Each Partner agrees to cooperate in the confirmation or other verification of the completeness and accuracy of any Operational Measures provided. At any time, each Partner agrees to cooperate with the Operational Committee in such requests, given reasonable prior Notice. The goal is for the

Partner to respond to a request within 24 hours; if the Partner cannot respond within 24 hours, the Partner shall request additional time to respond and such reasonable requests will be granted. If a Partner cannot in good faith provide Operational Measures as requested by the Operational Committee, the Partner may ask for relief from the request in writing to the Operational Committee.

2. **Execution of the E-MOU.** Each Partner shall execute this E-MOU and return an executed copy of this E-MOU to the Secretary of the Department of Innovation and Technology or designee. In doing so, the Partner affirms that it has full power and authority to enter into and perform this E-MOU. The Partner Executive shall be the representative authorized to sign on behalf of the Partner agency. The Partner Executive or designee shall maintain the E-MOU documents and make it accessible to all Partners, members of the Operational Committee, and any other stakeholders that the Secretary of the Department of Innovation and Technology or designee determines require access.

3. **Compliance with this E-MOU.** Except to the extent prohibited by Applicable Law, each Partner shall comply fully with all provisions of this E-MOU.

4. **Agreements with Users.** Each Partner shall have established agreements with each of its Users that require the User to, at a minimum: (i) comply with all Applicable Law; (ii) reasonably cooperate with the Partner on issues related to this E-MOU; (iii) Transmit Data only for a permitted purpose; (iv) use and disclose Data received from another Partner or User only in accordance with the terms and conditions of this E-MOU; (v) within 24 hours after determining that a Breach occurred, User will report such Breach to the Secretary of the Department of Innovation and Technology or designee and the State's Chief Information Security Officer, as well as following its agency's internal reporting procedures; (vi) refrain from disclosing to any other person any passwords or other security measures issued to the User by the Partner; (vii) sign the User Acknowledgement form found in Appendix 5, Attachment D; and (viii) cooperate with any external audits. Notwithstanding the foregoing, for Users who are employed by a Partner or who have agreements with the Partner which became effective prior to the Effective Date, compliance with this Section may be satisfied through written policies and procedures that address items (i) through (vi) of this Section so long as the Partner can document that there is a written requirement that the User must comply with the policies and procedures.

5. **Agreements with Vendors.** To the extent that a Partner uses vendors in connection with the Partner's Transmittal of Data, each Partner affirms that it has established agreements with each of its vendors, including ITSPs, that require the vendor to, at a minimum: (i) comply with Applicable Law; (ii) protect the privacy and security of any Data to which it has access; (iii) as soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Partner; (iv) not to re-disclose information without written consent of the Partner; (v) use information only for the purposes for which it was made available under the Business Purposes provided in the Specifications Sheet as described in Appendix 5; (vi) agree to the same restrictions on the access, use, and disclosure of Data as contained herein; (vii) reasonably cooperate with the other Partners to this E-MOU on issues related to this E-MOU; (viii) sign the User Acknowledgement form found in Appendix 5, Appendix D; and (ix) cooperate with any external audits.

6. **Creation of Test Data.** Certain Partners may agree to create Test Data (non-Individual/hypothetical data created for testing purposes only) to be used by other Partners for testing. Any Test Data shall not contain Production Data. Test Data shall be created in accordance with the Validation Plan and used only within a Test environment.

7. **Accuracy of Data.** When Transmitting Data, each Partner hereby represents that at the time of Transmittal, the Data it provides is (a) an accurate representation of the Data contained in, or available through, its System, (b) sent from a System that employs security controls that meet standards in accordance FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, provided in a timely manner and in accordance with the Specifications.

8. **Use of Data.** Each Partner shall use Data transmitted to it only in accordance with the provisions of this E-MOU and as permitted or required by Applicable Law.

9. **Requests for Data.** Data User shall notify the Operational Committee and the original Discloser Agency immediately when Data User receives a Freedom of Information Act Request, subpoena, court order or other third party request related to the Data. The Operational Committee, in conjunction with the Disclosure Agency, shall determine whether the information sought contains identifiable or confidential information and whether it shall be released. Data User shall refer all such communications to the Operational Committee and original Discloser Agency for their joint response and shall notify the requestor that the Data remains the property of the State. Nothing in this section shall require Data User to not comply with a valid court order.

10. **Compliance with Laws.** Each Partner shall fully comply with all Applicable Laws.

f. **Treatment of Data**. Each Recipient agrees to hold all Data in confidence and agrees that it shall not, during the term or after the termination of this E-MOU, re-disclose to any person or entity, nor use for its own business or benefit, any such Data obtained by it in connection with this E-MOU, unless such use or re-disclosure is permitted or required by Applicable Law and in accordance with the terms of this E-MOU. It is the responsibility of Recipients handling and processing data to ensure data is only used in compliance with the Business Processes listed in the Specifications sheet as described in Appendix 5. See Appendix 5, Attachment D.

g. **Disclaimers.**

1. **Reliance on a System.** Each Partner acknowledges and agrees that: (i) the Data provided by, or through, its System is drawn from numerous sources, (ii) the Data is specific to the point in time when drawn, and (iii) it can only confirm that, at the time of the Data Transmittal the Data are an accurate representation of Data contained in, or available through its System. Nothing in this E-MOU shall be deemed to impose responsibility or liability on a Partner related to the clinical accuracy, content or completeness of any Data provided pursuant to this E-MOU. The Partners acknowledge that other Partners' Digital Credentials may be activated or suspended at any time; therefore, Partners may not rely upon the availability of a particular Partner's Data.

2. **Carrier lines.** All Partners acknowledge that the Transmittal of Data between Partners is to be provided over various facilities and communications lines, and Data shall be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which may be beyond the Partners' control. Provided a Partner uses reasonable security measures, no less stringent than those directives, instructions, and specifications contained in this E-MOU and the Specifications and Applicable Law, the Partners assume no liability for or relating to the integrity, privacy, security, confidentiality, or use of any Data while it is transmitted over those carrier lines, which are beyond the Partners' control, or any delay, failure, interruption, interception, loss, Transmittal, or corruption of any Data or other information attributable to Transmittal over those carrier lines

which are beyond the Partners' control. Use of the carrier lines is solely at the Partners' risk and is subject to all Applicable Law. If a Breach occurs and it is determined that it happened because of a Carrier issue, the Partner responsible for the Data being transmitted is the responsible party for the Breach Notification. However, data should be encrypted using current industry standard algorithms agreed on by the parties involved before transmission occurs.

## ARTICLE IX
## TERM, ADDITION, SUSPENSION AND REINSTATEMENT

a. **Term.** The initial term of this E-MOU shall be for a period of one year commencing on the Effective Date. Upon the expiration of the initial term, this E-MOU shall automatically renew for successive one-year terms unless terminated by the Secretary of the Department of Innovation and Technology by providing to Partners at least ninety (90) days prior written notice of the termination of this E-MOU.

b. **Addition.** On-boarding new Data Exchange Services shall be in accordance with Appendix 1, Section 1 of this E-MOU.

c. **Suspension or Reinstatement.** Suspensions and Reinstatements of Data Exchange Services shall be in accordance with Appendix 1 (Sections 2, 3 and 4 respectively) of this E-MOU.

d. **Effect of Termination of Data Exchange Project.** Upon termination of a Data Exchange Services, and transfer of Data back to the Discloser (if requested by the Discloser), the Recipient is required to and shall purge all Data in its possession, including on computer hardware or software and in paper form. This purge must be performed in a manner no less restrictive than set forth in the requirements for "Purge" contained in NIST SP800-88, Appendix A: Minimum Sanitization Recommendation for Media Containing Data."

e. **Dispute Resolution Process.**

1. **General.** If any Dispute arises between Partners regarding the implementation of this E-MOU, those Partners agree to commence efforts to resolve such dispute in good faith via a designated subcommittee of the Operational Committee. The subcommittee will be formed by the Operational Committee within seven (7) business days after written notification of the Dispute. Any Partner may submit written notification of a Dispute to the Operational Committee. If the Disputed Matter has not been resolved by the subcommittee within thirty (30) days after first having been referred to the subcommittee (or at any earlier time, if requested by Partners who are parties to the Dispute), such Dispute may be referred to the Secretary of the Department of Innovation and Technology or designee for resolution.

2. **Activities during Dispute Resolution Process.** Pending resolution of any Dispute under this E-MOU, the Partners agree to fulfill their responsibilities in accordance with this E-MOU, unless the Partner is suspended by the Secretary of the Department of Innovation and Technology or designee.

3. **Implementation of Agreed Upon Resolution.** If, at any point during the Dispute Resolution Process, all of the Partners to the Dispute accept a proposed resolution of the Dispute, the Partners agree to implement the terms of the resolution in the agreed upon timeframe.

4. **Disputes between a Partner and the Operational Committee**. If any Dispute arises between a Partner and the Operational Committee, such Disputed Matter is escalated to the Secretary of the Department of Innovation and Technology or designee for resolution.

5. **Dispute Resolution before Suspension.** Partners agree to address differences using this Dispute Resolution Process as their initial method to resolve disagreements with other Partners. A good faith effort should be made proactively to resolve differences between Partners before the Operational Committee will consider interceding to recommend suspending a Partner from a Data Exchange Service for failing to fulfill their E-MOU defined duties.

6. **Appeal to the Chief Operating Officer.** If, following resolution of a Dispute by the State's Chief Information Officer, a Partner believes in good faith that the resolution would violate the Partner's legal obligations or be contrary to the best interests of the State, the Partner may submit the Dispute to the Governor's Chief Operating Officer (or another designee of the Office of the Governor). The Partner, the State's Chief Information Officer, and other interested persons shall provide information about the Dispute to the Chief Operating Officer upon request to enable a review of the Dispute and the initial resolution. The State's Chief Information Officer will revise the resolution as necessary upon direction from the Chief Operating Officer to ensure that the resolution complies with all legal obligations and is in the best interests of the State.

## ARTICLE X
## MISCELLANEOUS

a. **Notices.** All Notices to be made under this E-MOU shall be given in writing to the authorized Partner's representative at the address listed with the Operational Committee, and shall be deemed given: (i) upon delivery, if personally delivered or through the State's inter-agency mail system; (ii) upon the date indicated on the return receipt, when sent by the United States Postal Service Certified Mail, return receipt requested; and (iii) if by electronic Transmittal, upon the date and time of sending the Notice is directed to an electronic mail address listed with the Operational Committee.

b. **Governing Law.** This E-MOU shall be governed by and construed in accordance with the applicable laws of the United States and the State of Illinois.

c. **Amendment.** An amendment of the E-MOU may be recommended by agreement of at least two-thirds of the Operational Committee to submit to the Secretary of the Department of Innovation and Technology for his/her approval. All Partners agree to sign an amendment adopted in accordance with the provisions of this Section in accordance with Appendix1. Partners shall have the right to challenge an Operational Committee recommendation to amend the E-MOU, with the challenge being considered a Disputed Matter and resolved based on the Dispute Resolution Process described in Appendix Two of this E-MOU.

d. **Entire E-MOU.** This E-MOU, together with all Appendices and Attachments, constitutes the entire agreement. The official, executed version of this E-MOU shall be maintained in an electronic form by the Secretary of the Department of Innovation and Technology or designee. The Secretary of the Department of Innovation and Technology or designee shall maintain the E-MOU is a format that is accessible to all E-MOU Partners.

e. **Validity of Provisions.** In the event that any Section, or any part or portion of any Section of this E-MOU, is determined to be invalid, void or otherwise unenforceable, each and every remaining Section or part or portion thereof shall remain in full force and effect.

f. **Priority.** In the event of any conflict or inconsistency between a provision in the body of this E-MOU and any attachment hereto, the terms contained in the body of this E-MOU shall prevail.

g. **Headings.** The headings throughout this E-MOU are for reference purposes only, and the words contained therein may in no way be held to explain, modify, amplify, or aid in the interpretation or construction of meaning of the provisions of this E-MOU. All references in this instrument to designated "Sections" and other subdivisions are to the designated Sections and other subdivisions of this E-MOU. The words "herein," "hereof," "hereunder," and other words of similar import refer to this E-MOU as a whole and not to any particular Section or other subdivision.

h. **Relationship of the Partners.** Nothing in this E-MOU shall be construed to create a partnership, agency relationship, or joint venture among the Partners. Neither the Operational Committee nor any Partner shall have any authority to bind or make commitments on behalf of another Partner for any purpose, nor shall any such Partner hold itself out as having such authority. No Partner shall be held liable for the acts or omissions of another Partner.

i. **Effective Date.** With respect to the first two Partners to this E-MOU, the Effective Date shall be the date on which the second Partner executes this E-MOU. For all Partners thereafter, the Effective Date shall be the date that the Partner executes this E-MOU.

j. **Counterparts.** This E-MOU may be executed in any number of counterparts, each of which shall be deemed an original as against the Partner whose signature appears thereon, but all of which taken together shall constitute but one and the same instrument.

k. **Third-Party Beneficiaries.** There shall exist no right of any person to claim a beneficial interest in this E-MOU or any rights occurring by virtue of this E-MOU.

l. **Force Majeure.** A Partner shall not be deemed in violation of any provision of this E-MOU if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other disruptive natural occurrences; (c) power failures; (d) nuclear or other civil or military emergencies; (e) terrorist attacks; (f) acts of legislative, judicial, executive, or administrative authorities; or (g) any other circumstances that are not within its reasonable control. This Section shall not apply to obligations imposed under Applicable Law.

m. **Time Periods.** Any of the time periods specified in this E-MOU may be changed pursuant to the mutual written consent of the Secretary of the Department of Innovation and Technology and the affected Partner(s).

n. **Ownership**. Any Data provided by a Discloser to a Recipient shall remain the property of the Discloser even after it is provided to a Recipient. Recipient shall not obtain any right, title, or interest in the Data.

o. **Court Order or Subpoena**. In the event that any Data is required to be disclosed in response to a valid order to a court of competent jurisdiction or other governmental body of the United States or any political subdivisions thereof. Only the minimal necessary Data shall be

disclosed to the extent necessary and for the purposes of the court or other governmental body. The Partner will be notified of the order and provided with a copy of such order and Partner may seek a protective order.

p. **Public Notification**. If required by Applicable Law, Partner will post a copy of this E-MOU for public access.

## FERPA ADDENDUM

This Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99) ("FERPA") Addendum ("Addendum" or "FERPA Addendum") is an add-on to the State of Illinois Enterprise Memorandum of Understanding ("E-MOU"). It is applicable only in those situations where the Recipient obtains, transmits, uses, maintains, retains, processes, or disposes of Personally Identifiable Information (defined below) regarding students from the Illinois State Board of Education ("ISBE") in order to fulfill its obligations to ISBE pursuant to the E-MOU. ISBE is required by law to collect and store student records (105 ILCS 5/2-3.31), and takes seriously its obligations to secure information systems and protect the privacy of data collected, used, shared and stored by the agency. This Addendum sets forth the minimum requirements under the research and the audit or evaluation exceptions to FERPA. If any conflict exists between the terms of this Addendum and the E-MOU, the terms of this Addendum shall govern. If only de-identified data (defined below) will be used, this Addendum is not applicable (34 C.F.R. § 99.30).

## DEFINITIONS (34 CFR § 99.3)

*"Authorized representative"* means any entity or individual designated by a State or local educational authority or an agency headed by an official listed in §99.31(a)(3) to conduct—with respect to Federal- or State-supported education programs—any audit or evaluation, or any compliance or enforcement activity in connection with Federal legal requirements that relate to these programs.

*"Disclose", "disclosure"* or "*re-disclose*" means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record.

*"Education program"* means any program that is principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution.

"*Personally Identifiable Information*" ("*PII*") includes, but is not limited to— (a) The student's name; (b) The name of the student's parent or other family members; (c) The address of the student or student's family; (d) A personal identifier, such as the student's social security number, student number, or biometric record; (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

"*De-identified data*" means data that does not identify a particular individual, program, classroom, school, institution or district and with respect to which there is no reasonable basis to believe the data can be used to identify a particular individual, program, classroom, school, institution or district. Personally identifiable information has been removed or obscured from the data in a way that minimizes the risk of unintended disclosure of the identity of individuals, programs, classrooms, schools, institutions or districts and information about them whether through single or multiple releases, and taking into account other reasonably available information. 34 C.F.R. § 99.31(b)(1).

Recipient agrees to hold Confidential Student Information, which includes both PII and de-identified data subject to FERPA, in strict confidence. Recipient will not use or disclose Confidential Student Information received from or on behalf of ISBE except as permitted or

required by this Addendum, as required by law, or as otherwise authorized in writing by ISBE. ISBE has sole authority to authorize and approve data access and may limit the number of authorized contractors, subcontractors, or agents under this Addendum. Recipient must create and maintain a record of any disclosure of Confidential Student Information. The record of disclosure must record the name of any person or organization receiving the Confidential Student Information and their legitimate interest under 34 C.F.R. § 99.31 in requesting or obtaining the Confidential Student Information. Upon ISBE's request, Recipient must provide a copy of the record of further disclosures to ISBE. 34 C.F.R. § 99.32(b)(2)(i) and (ii).

**AUDIT OR EVALUATION EXCEPTION. 34 CFR *§§99.31(a)(3) and 99.35***

ISBE formally designates Recipient as its authorized representative for purposes of audit or evaluation of Federal- or State-supported education programs, or to enforce or to comply with Federal legal requirements that relate to those programs. The disclosure of the specified PII from education records is in furtherance of an audit, evaluation, or enforcement or compliance activity regarding such education programs. The specific PII being disclosed from education records is identified in Appendix 5 to the E-MOU and described therein with sufficient specificity to ensure that it falls within the audit or evaluation exception. Recipient will include a description of how the PII from education records will be used, the methodology and why disclosure of PII from education records is necessary to accomplish the audit, evaluation, or enforcement or compliance activity.

Recipient agrees to use the PII from education records only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with, Federal legal requirements related to these programs. Recipient agrees to protect the PII from education records from further disclosures or other uses, except as authorized by ISBE in accordance with FERPA. Approval to use the PII from education records for one audit or evaluation does not confer approval to use it for another.

Recipient will dispose of or return all Confidential Student Information to ISBE within ten (10) days, upon ISBE's request. All Confidential Student Information received pursuant to this Addendum shall be disposed of upon termination, cancellation, expiration, or other conclusion of the E-MOU. Disposal means the return of the Confidential Student Information to ISBE or destruction of the Confidential Student Information as directed by ISBE, including purging of all copies from the Recipient's computer systems. Upon disposal of the Confidential Student Information, Recipient will confirm to ISBE in writing the destruction of Confidential Student Information. Recipient agrees to require all employees, contractors, subcontractors, or agents of any kind to comply with this provision.

Recipient agrees to establish and maintain policies and procedures, consistent with FERPA and other Federal and State confidentiality and privacy provisions, to protect PII from education records from further disclosure and unauthorized use, including limiting use of PII from education records to only authorized representatives with legitimate interests in an audit, evaluation, or enforcement or compliance activity. Such policies and procedures will be described in Appendix 5.

**STUDIES EXCEPTION. 34 CFR *§99.31(a)(6)***

Recipient is an organization to whom ISBE can disclose PII from an education record of a student under the studies exception because the disclosure is to conduct studies for, or on behalf of ISBE, educational agencies or institutions to: (A) Develop, validate, or administer predictive tests; (B) Administer student aid programs; or (C) Improve instruction.

Recipient will specify in Appendix 5 the purpose of the study, describe its scope and duration and identify the information, including any PII, being disclosed. Recipient agrees to use PII from education records only to meet the purpose or purposes of the study.

Recipient will conduct the study in a way that does not allow personal identification of parents and students by individuals other than representatives of Recipient with a legitimate need to know, and will take steps to maintain the confidentiality of the PII from education records at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques.

Recipient agrees to destroy all PII from education records when the information is no longer needed for the purposes for which the study was conducted. ISBE will determine the specific time period for destruction based on the particular study.

IN WITNESS WHEREOF, the undersigned have caused this Agreement to be executed by their authorized representatives.

**ILLINOIS DEPARTMENT OF AGING**

_____
Jean Bohnhoff
Director

Date:_____

**ILLINOIS DEPARTMENT OF HUMAN SERVICES**

_____
James T. Dimas
Secretary

Date:_____

**CENTRAL MANAGEMENT SERVICES**

_____
Michael Hoffman
Director

Date:_____

**ILLINOIS DEPARTMENT OF INNOVATION & TECHNOLOGY**

_____
Hardik Bhatt
Secretary

Date:_____

**ILLINOIS DEPARTMENT OF CHILDREN & FAMILY SERVICES**

_____
George H. Sheldon
Director

Date:_____

**ILLINOIS DEPARTMENT OF JUVENILE JUSTICE**

_____
Candice Jones
Director

Date:_____

**ILLINOIS DEPARTMENT OF COMMERCE & ECONOMIC OPPORTUNITY**

_____
Sean McCarthy
Director

Date:_____

**ILLINOIS DEPARTMENT OF PUBLIC HEALTH**

_____
Nirav D. Shah, M.D., J.D.
Director

Date:_____

**ILLINOIS DEPARTMENT OF CORRECTIONS**

_____
John Baldwin
Director

Date:_____

**ILLINOIS STATE BOARD OF EDUCATION**

_____
Tony Smith
Superintendent

Date:_____

**ILLINOIS DEPARTMENT OF EMPLOYMENT SECURITY**

_____
Jeff Mays
Director

**ILLINOIS DEPARTMENT OF VETERANS AFFAIRS**

_____
Erica L. Jeffries
Director

Date:_____

**ILLINOIS DEPARTMENT OF HEALTHCARE & FAMILY SERVICES**

_____
Felicia Norwood
Director

Date:_____

# State of Illinois
# Enterprise Memorandum of Understanding (E-MOU)

# Appendices

# Appendix 1
# Procedures for Adding a New Partner and Suspending a Partner

## 1. Adding a New Partner

When an Applicant requests to join this E-MOU, the request shall be directed to the Chairperson of the Operational Committee in writing. As laid The Operational Committee shall vote on whether the requesting entity may join the eMOU at the next regularly scheduled Operational Committee meeting after the request is submitted and reviewed to ensure it conforms to the definition of Partner as specified in Article II of the eMOU. If the Operational Committee votes to accept the Applicant, the Applicant will be considered a Partner and shall execute this eMOU with its supporting appendices. The Chairman of the Operational Committee shall forward the approval of the new Partner to the State's Secretary of the Department of Innovation and Technology or designee and the Partner's General Counsel's Office and Chief Executive Officer.

If the Operational Committee does not approve the Applicant's request to become an eMOU Partner, the Operational Committee will so advise the Applicant, with specific reasoning as to why they are precluded from participation. .

## 2. 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 the State's Chief Information Officer or designee and members of the Operational Committee of the interruption prior to the interruption as early as possible but no later than one business day before the interruption, if planned (and Partner agrees that if planned, the interruption will occur outside of normal business hours if possible); or as soon as reasonably practicable after the interruption begins, if unplanned. The State's Chief Information Officer or designee shall simultaneously notify all other Partners 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 State's

# Appendix 1
# Procedures for Adding a New Partner and Suspending a Partner

Chief Information Officer and members of the Operational Committee 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. The State's Chief Information Officer or designee shall approve such Voluntary Suspension and simultaneously notify all other Partners of the voluntary suspension.

**B. With Cause**

If the Operational Committee finds that a Partner is in material default of the performance of a duty or obligation imposed on the Partner by this E-MOU, it shall recommend that the State's Chief Information Officer or designee notify the Partner, in writing as soon as possible but no later than 2 business days after the recommendation, 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 State's Chief Information Officer or designee, the Operational Committee may recommend that the State's Chief Information or designee suspend the Partner.

Additionally, the Operational Committee shall investigate all complaints, reports, or other information received regarding concerns that a Partner's information technology (IT) system is creating an immediate threat of Data Breach or will cause irreparable harm to another party, including, but not limited to, another Partner, a User, the Office of the State's Chief Information Officer, or an Individual whose Data is exchanged pursuant to this E-MOU. The Operational Committee shall notify the State's Chief Information Officer or designee of any recommendation that such Partner be issued a finding requiring a corrective action plan to remedy the issue for the specific IT System.

When the complaint, report, or other information indicates that a suspension from receiving data to a Partner's specific IT system must be implemented immediately and, in the judgment of the Chairperson, it is not practical to delay the suspension until the Operational Committee is convened, the Chairperson shall immediately:

- take all technical actions necessary to carry out the suspension including, but not limited to, suspension of the Partner's Digital Credentials to receive, but not provide, data to E-MOU Partners from the IT system in question;

# Appendix 1
# Procedures for Adding a New Partner and Suspending a Partner

- call a special meeting as soon as possible of the Operational Committee to evaluate the recommendation of suspension; and
- notify the suspended Partner of the suspension (as well as the other Partners of the decision).

The investigation by the Operational Committee discussed above may follow the immediate action.

If the Chairperson determines that immediate suspension is not required, the Operational Committee may initiate an investigation of the complaint, report, or other information. The Operational Committee Chairperson shall immediately notify the Partner(s) in question of the investigation.

The Operational Committee shall meet as soon as practicable, but no later than five (5) business days after the receipt of the complaint by the Operational Committee, to evaluate the suspension action by the Chairperson. The suspension shall remain in effect until the Operational Committee meets to evaluate the suspension and makes a recommendation to the State's Chief Information Officer or designee to affirm, modify, or terminate the suspension.

If the Chairperson of the Operational Committee is, or reports to, an employee of the Partner identified by the complaint, the Chairperson shall recuse himself/herself from the investigation of the complaint and defer complaint oversight duties to the Vice-Chairperson.
If a complaint is referred to the Chairperson and such complaint has not been resolved by the Operational Committee within thirty (30) days after it was first referred to the Chairperson (or such longer period as agreed to in writing by the Partners who are parties to the compliant), then the complaint shall be escalated to the State's Chief Information Officer or designee for resolution. If the State's Chief Information Officer or designee cannot reach a decision within five (5) business days from the referral or does not state that an additional five (5) business days is necessary to reach a decision, then the complaint is dismissed with no action taken against the Partner.

If, through the investigation, the Operational Committee recommends 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, the Office of the State's Chief Information Officer, or an individual whose Data are exchanged pursuant to the E-MOU, the Operational Committee may recommend to the State's Chief Information Officer or designee that such Partner be issued a finding requiring a corrective action plan to remedy the issue for the IT system. If the State's Chief Information Officer or designee concurs in the recommendation, the State's Chief Information Officer or designee shall take all technical actions necessary to carry out the finding or suspension including, but not limited to, suspension of the Partner's Digital Credentials to receive data from, but not provide data to E-MOU Partners from the IT system in question. As soon as reasonably practicable after suspending a Partner, but in no case longer than twelve (12) business hours, the Operational Committee Chairperson, with the concurrence of and through the Office of the States' Chief

# Appendix 1
# Procedures for Adding a New Partner and Suspending a Partner

Information Officer, 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 Operational Committee with a written plan of correction or an objection to the suspension within five (5) business days of being notified of the suspension.

Any objection shall specify the reason that the Partner feels the suspension is inappropriate. The plan of correction shall detail the action that the Partner is taking to address, mitigate and remediate the issue(s) that were the basis for the suspension as outlined in the summary and include a timeframe for such actions. The Operational Committee shall meet and review a suspended Partner's plan of correction or objection within five (5) business days of receipt from the Partner; determine whether to recommend to the State's Chief Information Officer or designee to accept or reject the plan of correction or affirm the suspension; and communicate such decision to the State's Chief Information Officer or designee who will act on such recommendation and provide his/her decision to the subject Partner and the Operational Committee.

If the Operational 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 Operational Committee and the suspended Partner cannot reach agreement on the content of the plan of correction or on the reasons supporting the suspension, the Operational Committee may submit the Dispute to the State's Chief Information Officer for resolution.

Any suspensions imposed shall remain in effect until the Partner is reinstated with this E-MOU.
A finding requiring a Corrective Action Plan, but not a suspension, shall describe the action that the Partner is taking to address, mitigate and remediate the issue(s) that caused the Operational Committee to make the finding and include a timeframe for such actions. The Partner's corrective action plan in response to an Operational Committee finding shall be submitted within thirty (30) days of the finding being issues. The Operational Committee shall meet and review a Partner's corrective action plan at the next regular meeting following the submission of the corrective action plan from the Partner; determine whether to recommend to the State's Chief Information Officer or designee to accept or reject the plan; and communicate such decision to the State's Chief Information Officer or designee who will act on such recommendation and provide his/her decision to the Partner and the Operational Committee no later than five (5) business days after receipt from the Operational Committee.

**3. Reinstatement**

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

# Appendix 1
# Procedures for Adding a New Partner and Suspending 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, the State's Chief Information Officer or designee shall take all technical actions necessary to reinstate the Partner's ability to participate in the Data Exchange Service including, but not limited to, the reinstatement of the Partner's Digital Credentials.

**B. After Suspension with Cause**

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

If the Operational Committee is not satisfied that the Partner has met its obligations under its plan of correction, the Operational Committee Chairperson shall inform the Partner of the deficiencies within five (5) business days of reaching that decision. The Partner will have the ability to submit additional evidence that addresses such deficiencies

When the Operational Committee is satisfied that the evidence presented indicates that the Partner has fulfilled its obligations under the plan of correction, it shall recommend that the State's Chief Information Officer take all technical actions necessary to reinstate the Partner's ability to participate in the Data Exchange Service including, but not limited to, the reinstatement of the Partner's Digital Credentials. Such action should be completed as soon as possible but not later than three (3) business days after reaching that decision. The State's Chief Information Officer, or designee, shall inform all the Partners of such reinstatement forthwith.

# Appendix 2
# Process to Amend the E-MOU

## 1. Submission of Proposed Amendments to the E-MOU

Any Partner may submit in writing to the Operational Committee Chairperson 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 desired;
- the proposed language for the requested amendment; and
- an analysis of the expected impact of the requested amendment.

## 2. Consideration of Proposed Amendments to the E-MOU

If, after considering the request at the next regularly-scheduled meeting, the Operational Committee determines that the request does not have merit, it shall communicate this determination to the requesting Partner.

If, after considering the request at the next regularly-scheduled meeting, the Operational Committee determines that the request has merit, the Operational Committee shall forward the request to the State's Chief Information Officer or designee to seek approval of the recommended amendment. When the Operational Committee seeks approval of such amendments, the Operational Committee shall provide the State's Chief Information Officer or designee with the following information:

- a copy of the proposed amendment to the E-MOU;
- description of why the requested amendment is desired and any foreseeable impact of the amendment;
- statement regarding whether the proposed amendment is necessary in order for the Operational Committee or Partners to comply with Applicable Law; and
- projected effective date for the proposed amendment.

If the State's Chief Information Officer or designee agrees with the proposed amendments to the E-MOU, the State's Chief Information Officer or designee will advise all of the Partners of such decision and the effective date for the proposed amendment.

## 3. Approval or Rejection of Proposed Amendments to the E-MOU

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

Once an amendment is recommended by the Operational Committee, and the State's Chief Information Officer agrees with the recommendation, all Partners are advised to sign the amendment to the E-MOU prior to the effective date of the amendment.

# Appendix 3
# Change Process for Data Exchange Services

## 1. Requests for Change

### A. Development Changes

The Operational Committee shall have the authority to adopt new E-MOU Service Specifications or Specification of Service and use of Emergent Specifications, and to adopt amendments to, or repeal and replace, the E-MOU Service Specifications or Specification of Service (collectively a "Development Change"). Service Specifications must conform to those found in Appendix 5 of this E-MOU.

### B. Compliance Changes

The Operational Committee shall have the authority to recommend to the State's Chief Information Officer to adopt new or to make Changes to existing E-MOU Service Specifications or Specification of Service that are necessary: (1) for 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 Operational Committee, a task group may evaluate the Change and provide comments to the Operational Committee.

## 2. Receipt

All requests for Changes shall be directed in writing to the Operational Committee Chairperson. The Operational Committee Chairperson shall catalog all requests for Changes upon receipt.

The catalog shall include:

a. Type of the proposed change (*e.g.* new, amendment, repeal)
b. Name and version number of the specification;
c. Whether the proposed change is a Development Change, Compliance Change or a request for consultation;
d. 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);
e. Description of the actual changes;
f. Preliminary analysis of the potential business and technical impact to Partners and their Users;
g. Copy of the Specification; and
h. Requesting agency and date of request.

The catalog will be made available online.

# Appendix 3
# Change Process for Data Exchange Services

## 3. Evaluation

The Operational Committee shall, within thirty (30) business days after being informed by the Chairperson of receipt, forward the request for change to a task group designated by the Operational Committee for technical evaluation of the request and to make a recommendation to the Operational Committee. During consideration of the request for change, the task group may request additional information from the Operational 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 Operational Committee Chairperson shall ensure each Partner is provided a copy of the original proposed Change. Each Partner shall respond in writing to the Operational Committee Chairperson by a designated response date with the following information:

a. whether the implementation of the Development Change will have a significant adverse operational or financial impact on the Partner;
b. whether implementation of the Development Change will require the Partner to materially modify its existing agreements with its Users or third parties;
c. whether the Partner believes that implementation of the Development Change will require an amendment to the E-MOU, including amendments to the permitted purposes; and
d. whether the Partner would implement a change (if optional). and
e. whether the implementation would potentially violate applicable law and a description of the potential violation.

The Partner agrees to provide rationale for each affirmative response. The task group or the Operational 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 Operational Committee about the proposed change. Factors in considering the proposed change shall include:

a. whether the change has a significant adverse operational or financial impact on at least 20% of Partners;
b. whether the change requires at least 20% of Partners to modify their existing

agreements with Users or third parties;

c. whether the proposed change requires an amendment to the E-MOU; and
d. whether the proposed change may violate applicable law.

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

If a new Agency 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 Operational Committee at the Operational Committee's next regularly scheduled meeting following the designated response date. The Operational Committee shall review the task group's recommendation and make a final recommendation to the State's Chief Information Officer regarding whether the Development Change should be approved.

**3. Evaluation of Compliance Changes.**

If the proposed Change is a Compliance Change, the task group shall review the Change to assess its impact. The task group shall meet with the Operational Committee and present its findings and recommendations on the Compliance Change within three (3) weeks of the task group receiving the proposed Compliance Change. The Operational Committee shall review the task group's recommendation and make a final recommendation to the State's Chief Information Officer or designee 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 Operational Committee regarding 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 Operational Committee shall provide an opportunity for affected Partners to provide feedback on their preferred timeline and ability to absorb the additional work required by any changes. The task group shall consider:

a. Whether the Change impacts interoperability among the Partners;
b. The number of versions of the Specification that will be supported for backward compatibility purposes and the business implications of such support;
c. If multiple versions will be supported, a sunset date for such support as the multiple versions are collapsed;
d. The business implications for Partners related to migrating to the new Specification;

e. The number of Partners and number of transactions that will be impacted by the new Specification;
f. The amount of time that Partners should be given to migrate to the new Specification;
g. Whether legislative or regulatory changes are required;
h. The time it will take to conduct a security review of the changes with the State's CISO; and
i. Sunset dates as "old" specifications are retired.

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

**B. Response**

1. **Development Changes.**

At the conclusion of the response period established during the evaluation of the proposed Change, the Operational Committee shall evaluate whether to recommend to the State's Chief Information Officer that the Development Change be approved, if revisions to the E-MOU will be required and a proposed timeline for implementation. The recommendation of the Operational Committee regarding the Development Change and the proposed timeline for implementation shall be communicated to the State's Chief Information Officer or designee. Revisions to the E-MOU necessitated by approved Development Changes will be performed in accordance with Appendix 2 of this E-MOU.

2. **Compliance Changes.**

Based upon responses from the Partners, the Operational Committee shall provide input to all Partners on the impact of the Compliance Change and the recommended timeline for implementation.

# Appendix 4
# Procedures for Breach Notification

## 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 State's Chief Information Officer or designee and the Chief Information Security Officer. Such reports shall be made within 24 hours from when the Partner discovered or should have discovered the occurrence. Partners shall also comply with any Applicable Law regarding Breaches.
2. Following this Notification to the State's Chief Information Officer or designee and the Chief Information Security Officer, the Partner(s) shall immediately provide Notice to the members of the Operational Committee by sending an email to the Operational Committee Chairperson.
3. The Operational Committee will develop detailed notification instructions for specific types of breaches (for example, FTI, SSA, FPLs) involving Individual confidential or protected information. These instructions will include procedures to work with privacy officers regarding compromised Data. Once developed, these detailed notification instructions shall be submitted to the State's Chief Information Officer for his/her approval. Once approved, these instructions shall be incorporated into this Appendix and will be followed accordingly.

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

### B. Notification Content

The Notification shall include sufficient information for the Operational 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.);
- the specific Data or Type of Data that is the object of the Breach;
- partners likely impacted by the 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
- corrective action taken and steps planned to be taken to prevent a similar Breach.

# Appendix 4
# Procedures for Breach Notification

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 future website and directed to the same addresses used for the original 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 1 of this E-MOU.

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

**A. Review of the Breach by the Operational Committee**

The Operational Committee Chairperson shall facilitate a meeting of the Operational Committee upon receipt of the Breach alert or Notification as soon as practicable for the purpose of reviewing the Notification and determining the following:

1. the impact of the Breach or potential Breach on the privacy, security, confidentiality and integrity of the Data Transmittals;
2. whether the Operational Committee needs to take any action to suspend the Partner(s) involved in the Breach or potential Breach in accordance with Appendix 1 of the E-MOU;
3. whether the Operational Committee should take any other measures in response to the Notification or alert.
4. the Operational Committee shall, if needed; request additional information from the Partner(s) involved in the Breach or suspected Breach to fulfill its responsibilities. However, with respect to suspected Breach alerts, the Operational 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 whether a suspected Breach is indeed 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. Determination of Breach Resolution**

Once complete information about the Breach becomes available, the Operational Committee shall meet as soon as possible to determine whether the Corrective Actions taken by the Partner(s) involved in the Breach are sufficient to mitigate the Breach and prevent a similar Breach from occurring in the future. Once the Operational Committee is satisfied that the Partner(s) have taken all appropriate measures, the Operational Committee shall deem the Breach resolved and will so advise the State's Chief Information Officer or designee of such recommendation. Upon renewal of any Data Requests, Partners shall list any data breaches that occurred in the previous twelve (12) months and provide an updated status on any corrective action plan arising from the breach.

# Appendix 4
# Procedures for Breach Notification

1. 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.
2. If those Partners do not resume Data Transmittals with the Partner(s) involved in the Breach within a reasonable period of time and no longer than ten (10) business days after the resolution was communicated, the Partner(s) involved in the Breach and cessation shall engage in the Dispute Resolution Process with the State's Chief Information Officer in accordance within this E-MOU.
3. Lessons learned on the root cause of the Breach will be communicated by the Operational Committee to all Partner(s), including those not involved in the Breach, to prevent a recurrence of the event in the future.

# Appendix 5
# Requirements for Data Exchange Services

Each Data Exchange Service must identify details specifying the business need, data content, security expectations, availability and dependency requirements. Those requirements are outlined in the section that follows. In addition, each Data Exchange Service must be validated according to testing requirements as identified in Appendix 6 of this E-MOU.

## 1. Specifications for New/Revised Data Service.

Data Exchange Services are generally the transmission and transformation of data. The latency can range from near real-time to regularly schedule batch file processing. The records layout can be fixed length, with each byte in the file having a pre-determined meaning, or can be variable length with delimiters. The mode of transportation should always be secure, but can be done via web-services or secure modes such a SFTP. These options will be driven by the needs of the business use of the Data Service.

### A. Process for Requesting New/Revised Data Exchange Services

i. Applicant must complete and submit an E-MOU Data Service Request Form, which can be found in Attachment A to this Appendix, to the Operational Committee. Applicants shall use this template upon an initial request or revision of data from Partners in accordance with the E-MOU. The eMOU Operational Committee shall submit all Data Requests to the General Counsel's Office of the Agency from which the requested Data originates as specified in Article VIII of this eMOU.

ii. The Operational Committee shall review new or revised data service requests at their next regularly scheduled meeting after the data service request is made. If the data service request is approved, the Operational Committee will contact the Applicant and request they complete and submit the E-MOU Internal Control Questionnaire ("ICQ"). (ICQ is only required if Partner is receiving Data; not required if solely sending data.) The ICQ can be found in Attachment B to this Appendix. Applicants shall use this template to request or revise a data service request in accordance with Appendix 2 of the E-MOU.

1. The Operational Committee shall conduct an initial review of new or revised ICQ within thirty (30) days of their submission and shall make a determination within said thirty (30) days, and no longer than ninety (90) days from date of submission as described below in this paragraph. If no initial review has occurred within thirty (30) days of submission to the Operational Committee, the ICQ shall be approved. Upon initial review of the ICQ, the Operational Committee may request clarification or additional information from the Applicant within thirty (30) days of the submission. Clarification and/or additional information shall be provided back to the Operational Committee within thirty (30) days of the request. Review of an ICQ shall take no longer than ninety (90) days in total, however, the Applicant may request an extension of the review period from the Operational Committee in writing before the ninety (90) day review period expires.

2. If the ICQ is approved, the Applicant shall begin to draft a Specification Sheet as well as any necessary User Confidentiality Agreement Acknowledgement Form*. (If only sending data, there is a different Specification Sheet required and no User Confidentiality Agreement Acknowledgement Form is required.) A Specification Sheet can be found in Attachment C to this Appendix. A User Confidentiality Agreement Acknowledgement Form can be found in Attachment D to this Appendix.

***The requesting entity is required to have each person who is authorized to access the data sign a User Confidentiality Agreement Acknowledgement form**

**B. Specification Sheet**

1. **Data Service Name**
   Name the service in a business friendly fashion. Describe so it is clear what type of business function is being performed. Like services should be named in a consistent method to enable reuse and effective management.
2. **Statement of Business Purpose**
   Describe the business purpose of the Data Service in terms that existing Partners, the Operational 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.
3. **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 functional and non-functional requirements. 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
      - Code – A limited set of valid values

   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
      - Citizen –was provided by a Citizen or User

# Appendix 5
# Requirements for Data Exchange Services

- Partner – sourced from a State Agency, either active or inactive with the Exchange
- 3rd party –is provided by an external third party entity, not affiliated with any state Agency
- SSA – field content came from the Social Security Administration
- IRS – field content came from the Internal Revenue Service
- 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
- ($##.####) – 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. Typically this represents the user's sensitivity of the content. 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 Illinois and federal 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

vi. Validation – Detail what data checking routines will be put in place to ensure (i) message format and content are valid and (ii) content has been received without error.

4. **Delivery Model**

# Appendix 5
# Requirements for Data Exchange Services

Does this service send (push) Data to others or does the service receive (pull) Data from others? Identify which model the service typically operates under. Document any business requirements or assumptions for the event that triggers the data service.
Document if any logic exists to support restarting the service should the transfer fail unexpectedly. Include details on how to initiate the restart process.

Define details on the data transfer process. Trace the business path of the data transfer from source system to target location. Identify if any updates or transformations are made to the data in transit. Capture details on the transport protocol that will be applied transferring the data. Note if the transport protocol changes along the path. Also indicate the transfer/transmittal protection requirements to ensure the Data content is protected appropriately per Applicable Law.

5. **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 Partner-specific technical implementation standards.

Define format details about the service. What type of file is being processed: XML, CSV, Fixed Format. Record if the file includes a header and/or footer row and the supporting details.

Define any validation necessary to confirm complete transmission of the service. These validations may include check-sums, record counts, or total matching with header/footer.

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

The data service should be classified as to whether it is considered to be a 'full-refresh' (ignore everything previously transmitted), a 'delta' (This updates the data this service has previously supplied), or 'append' (An addition to everything previously supplied). Some services may require that multiple options be available at certain times such as a normally provide a 'delta' but in the circumstance where the data becomes out of sync, do a 'full-refresh'.

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.

# Appendix 5
# Requirements for Data Exchange Services

6. **Security Requirements**

Identify if the data service must comply with specific security requirements (State or Federal) because it transmits protected content such as Protected Personally Identifiable Information (as defined by State Law) or Protected Health Information (as defined by Federal Law). Identify the business requirement that mandates such protected information be transmitted. Reference Partner System Security Plans, policies and procedures 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, the data may be shared only 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 should include requirements stipulated by Applicable Law.

Authorized transmissions should contain language regarding manipulation of data or files, authorization prior to transmission and use of message authentication codes.

Confirm that Applicable Law has been reviewed and if existing Data Exchange Authorization language 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.

7. **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.

8. **Related Service Dependencies**

# Appendix 5
# Requirements for Data Exchange Services

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.

9. **On-boarding Validation Plan**

Outline the strategy and plan to validate a Partner's successful integration and use of a data service. The On-boarding Validation Plan should define the approach on how to on-board an Applicant 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. This plan shall be reviewed and amended, as necessary, by the Operational Committee.

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.
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.
    - Dependencies – test case serves to validate that prior dependencies, if any, have been met.
iv. Expected Results – description of the expected results of the test case.
v. Once a test case passes, the output should be stored to automate future regression testing. Each time a result is modified the output must be updated.

# Appendix 6
# New Partner Testing and Validation Requirements

This section describes the testing activities to be performed by a potential Partner new to the Data Exchange Services or an existing Partner wishing to access new Data Exchange Services (referred to as Applicant). The Operational Committee shall develop the Testing environments that will include the necessary security controls sufficient to protect the sensitivity of the Data. Once developed, such Testing environments shall be included as an Appendix herein.

The process for Applicants to join the Data Exchange Services is described in Appendix 1 of this E-MOU.

**A. Select Services to Adopt**

i. The Applicant must complete and submit an E-MOU Data Service Request Form. See Appendix 5, Section 1(a)(i). (Step #1)
ii. The Operational Committee shall review new or revised data service requests at their next regularly scheduled meeting after the request is made. See Appendix 5, Section 1(a)(2). (Step #2)
iii. If the data service request is approved, the Operational Committee will contact the Applicant within five (5) working days and request they complete and submit the E-MOU Internal Control Questionnaire ("ICQ"). See Appendix 5, Section 1(a)(2). (Step #3). (If only moving data into an HHSi2 data environment, and Partner is not considering receiving data, then this will not be a required step.)
iv. If the ICQ is approved, the Applicant shall begin to draft a Specification Sheet as well as any necessary User Confidentiality Agreement Acknowledgement Form. See Appendix 5, Section 1(a)(3) (Step #4). (If only moving data into an HHSi2 data environment, and Partner is not considering receiving data, then this step will not be required.)
v. The Operational Committee shall conduct an initial review of new or revised ICQ within thirty (30) days of their submission. See Appendix 5, Section 1(a)(4). (Step #6)
vi. If no concerns are identified (Step #5), the Applicant is approved to begin testing.
vii. State's Chief Information Officer will schedule and activate the selected services for the Applicant in the development environment (Step #7) within ten (10) business days.
viii. Applicant Partner may begin testing with the selected services in the development environment (Step #8).

**B. Conduct Tests**

i. Testing can be conducted using the approved Enterprise automated testing tools, or performed manually by the Applicant Partner.
ii. Testing will focus on peer-to-peer testing of the Applicant Partner's system against an implementation of the selected service(s) in the target environment (Step #9).
iii. Validation is concerned with confirming that the interactions occur successfully as described by the selected service(s) on-boarding Validation Plan. Data Service Request Validation requires data checking routines that ensure (i) message format and content are valid; (ii) content has been received without error; (iii) header and trailer record counts match the data received.

iv. Testing will be accomplished by performing the test cases as identified in the selected service(s) on-boarding Validation Plan, and capturing the evidentiary artifacts defined in the on-boarding Validation Plan to enable review by the Operational Committee (Step #10).

**C. Report Test Results**

Although the Operational 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 Operational Committee (Step #10), accompanied by logs, screen shots, and other evidentiary artifacts as identified in the selected service(s) on-boarding Validation Plan.

**D. Validation**

i. The Operational Committee will review the produced evidence, consulting within its internal membership as needed.
ii. The Operational Committee will provide an opinion of the Applicant test report within ten (10) business days from submission (Step #11).
iii. With approval from the Operational Committee, the Applicant may proceed to the next environment in the promotion sequence (Step #12).
iv. If the Operational Committee does not approve the Applicant test report, the Operational Committee will advise the Applicant with specific remediation guidance to improve compliance when re-testing (return to Step #9).
v. The workflow is repeated by the Applicant for development, testing, training and User acceptance testing environments. Each must be performed in sequence.
vi. Once the Applicant has successfully completed the User acceptance testing, the Applicant test results will be reviewed by the Operational Committee for production environment access (Step #13) and recommendation to the State's Chief Information Officer regarding a Partner's authority to send and/or receive or have access to Data. (Step #14).

# Attachment A to Appendix 5
# New Partner Testing and Validation Requirements

In the course of administering the Illinois state programs and related service activities, Illinois State Agencies collect information from individuals, employers and providers. Some of that information is public; most is confidential. Information that identifies a person or an employer is protected in Illinois in accordance with stringent state and federal laws. Those laws allow Illinois State Agencies to release some confidential information if the request or requestor meets specific requirements.

Complete and submit the following application in order to be considered for legal access to certain confidential data collected by the State. Please note the required fields below, indicated with a red asterisk:

* Required

---

Legal name of the requesting entity: *

Legal name of the owner entity: *

Name of Preparer or Contact Person: *

Contact Email Address: *

Contact Phone Number (primary): *

Street Address: *

City *

State *

Zip Code *

What specific data points are you requesting? Please include a description of the data points. *

How do you intend to use the data? *

At which location(s) will the data be used? Please include the specific address(es). *

If required or permitted by applicable law, under what legal authority would you like to obtain access to the data? Please include any specific law and/or citation. If no law restricts access to this Data, please respond N/A. *

How many staff will be accessing the data? Please include a listing of the specific individuals. *

# Attachment A to Appendix 5
# New Partner Testing and Validation Requirements

Do you intend to share the data with subcontractors? Please include a listing of the specific subcontractors. *

**Additional questions specific to the data or Agency from which the request is being made:**

*(For Agency staff only: please add additional questions required by state or federal law managing the dissemination of this specific information type.)*

# Attachment B to Appendix 5
# Internal Control Questionnaire

INSTRUCTIONS

The following questions serve as the Internal Control Questionnaire for the Applicant Partner's security procedures relating to the E-MOU documents and electronic media as part of the E-MOU contractual requirements.

When answering the questions in this document, the answers should be entered on the line directly below the question.

After completion, the form should be printed out and signed by the Disclosure Officer and the Director from the Agency.

The Agency should complete the contact information below for all parties involved in supplying information.

| Name | Title | E-mail |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

It is advisable for the Applicant Partners to collect and maintain documented evidence to back up answers to this report in the instance of an audit.

A. General Information

1. Do you currently utilize an E-MOU data service?

    a. If yes, please describe the type of data and what format the data is in? (paper documents, electronic media, etc.)

# Attachment B to Appendix 5
# Internal Control Questionnaire

2. How is data received? (Tumbleweed, ConnectDirect, other Secure Data Transmission (SDT)-list)

3. Are paper documents or electronic media created from the E-MOU data (letters, reports, etc.)? If yes, please describe what paper documents or electronic media are created.

4. How are the paper documents or electronic media distributed?

5. Are any paper documents or electronic media provided to a contracted State Agency or Contractor? (e.g., consolidated storage center, offsite storage location)

    a. If yes, please provide the Site Name and Address for each facility that house E-MOU paper documents or electronic media.

6. What safeguard controls are in place when transmitting and processing the E-MOU paper documents or electronic media at these locations?

7. Where are E-MOU paper documents or electronic media stored before and after processing at these locations? (Agency, Data Center, Other-list)

8. For E-MOU electronic media, do you keep back-up files? If so, how are data files backed up, by whom, and on what type of media?

9. For E-MOU electronic media, what is the retention period of back-up media and how many generations of back-up files exist at this time?

B. Security

**I.** Physical Security

10. Please describe the physical security of the Applicant Partner's Headquarters and any State Agency and/or User? (E.g. keypad locked doors, alarm systems, guard desks, locations, hours, etc.)

    a. If keypads are used, is each attempt logged? Who reviews the access logs? (Name and title)

    b. Who monitors any alarm systems? (e.g. Intrusion Alarms, Security Cameras, Motion Detectors, Exit Alarms) (Name and title)

# Attachment B to Appendix 5
# Internal Control Questionnaire

11. Are all paper documents or electronic media containing E-MOU data and devices through which E-MOU data is received, stored, processed, or transmitted at these facilities locked or otherwise secured? (e.g., restricted access server room, locked server rack, restricted access media library)?

    a. If yes, please describe how they are locked or secured, including key control procedures, and/or combination lock control procedures for each separate facility.

12. Is E-MOU data transmitted via fax machine?

    a. Where is the receiving fax machine located? (location in office)

    b. Are all individuals in the receiving location authorized to access E-MOU data?

13. For each facility, do visitors/vendors sign a visitor access log?

    a. If yes, what information is captured on the log? Where is the log stored and for how long?

14. Who has access to the Data Center at the Applicant Partner's Headquarters and any State Agency or User contracted with by the requesting Agency after core business hours? (Name and Title)

    a. How is security enforced after core business hours?

**II.** Application Security

Partner should supply information in "Section II. Application Security" ONLY if they store or process E-MOU electronic media in Agency applications.

15. Are application users supplied with unique user IDs?

    a. How does the user receive their user ID?

    b. Are accounts configured to lock after 3 failed login attempts?

    c. Are user IDs disabled after 90 days of inactivity?

16. Is the application configured to lock/terminate the session after 15 minutes of inactivity?

17. Does the Partner track and document application security incidents on an ongoing basis?
18. Is E-MOU data transmitted via email?

a. How is the data protected? (encryption - describe)

19. Does the Partner have web-based applications?

    a. Is E-MOU data accessible through a web site?

20. What software and version is used for Virus Protection?

21. What software and version is used for Spam/Spyware Protection?

22. What software and version is used for Intrusion Detection?

23. Does the Partner provide annual security awareness training regarding the handling of confidential data? If yes, please describe.

    a. Are there records maintained to track employee completion of this training?

C. Restricting Access

24. Is E-MOU electronic media kept separate or is it commingled with other information?

25. Can E-MOU paper documents or electronic media within agency records be located and separated easily?

26. How is access limited to authorized personnel?

D. Disposal

27. Is paper waste material with E-MOU data generated?

    b. How is the paper waste material destroyed? (recycle bins, locked containers, waste baskets, other container)

    c. Is a contractor used to pick up the paper waste material?

        i. If yes, please provide the name of contractor:

        ii. Where does the contractor take the paper waste material for destruction?

# Attachment B to Appendix 5
# Internal Control Questionnaire

E. Additional questions specific to the data or Agency from which the request is being made:

*(For Agency staff only: please add additional questions required by state or federal law managing the dissemination of this specific information type.)*

I acknowledge that I've been presented and reviewed the responses laid out here in the Internal Controls Questionnaire as a part of the E-MOU contractual requirements.

*/s/*

_____ _____

Disclosure Officer Date

*/s/*

_____ _____

# Attachment C to Appendix 5
# Specification Sheet for a Data Service

**A. Data Service Name**

| |
|---|
| *Define a user friendly name*<br>*ex: DMV_ValidateCitizenIdentity* |

**B. Statement of Business Purpose**

| |
|---|
| *Single short paragraph to define the business purpose of this service* |

**C. Business Data of the Service**

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

**D. Delivery Model**

Is this a push vs. pull interface? (Select one)

| | |
|---|---|
| *Yes or No* | Sends data (push) when triggered |

# Attachment C to Appendix 5
# Specification Sheet for a Data Service

| | |
|---|---|
| *Yes or No* | Provides data (pull) when requested? |

Define business requirements to trigger the interface

| |
|---|
| *Short paragraph that defines the triggering event for the service* |

Required transport mechanism

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

**E. Physical Designation of the Service**

Where can the physical description be found?

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

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

| |
|---|
| *Define which standard aligned with or define why the service is now aligned.* |

What format is the physical interface defined with?

| |
|---|
| *Define – MQ, WSDL, other based* |

Logging Requirements

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

Archiving Requirements

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

**F. Security Requirements**

Does this interface require specific security requirements?

| |
|---|
| *Describe special security handling because of PII, PHI, PCI, HIPAA, HITECH, SSA, IRS content* |

Should this interface only be available to a subset of Partners and/or Users?

| |
|---|
| *If so – define parties to include or exclude; be clear.*<br>*Cite the Federal/State code that mandates this limitation* |

Will the interface require additional citizen consent?

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

**G. Service Level Agreements**

Availability of service

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

BC/DR requirements

# Attachment C to Appendix 5
# Specification Sheet for a Data Service

| |
|---|
| *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.* |

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?* |

Performance/response time expectations

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

**H. Related Service Dependencies**

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

| **Name of related service** | **Define the relation to this service** |
|---|---|
| *Name of related service* | *Is it essential/compulsory as a required predecessor or invoked as a sub-service?* |
| | |

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.* |

**I. Additional Questions Specific to the Data or Agency from which the Request is Being Made.**

*(For Agency staff only: please add additional questions required by state or federal law managing the dissemination of this specific information type.)*

**J. On-boarding Validation Plan**

# Attachment C to Appendix 5
# Specification Sheet for a Data Service

Test Objective

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

Testing time

| |
|---|
| *Specify the length of time needed for testing activities* |

Resources Needed

| |
|---|
| *Specify the resources needed from Operational Committee members, members of DoIT, etc. to conduct and complete testing activities* |

Testing Environment

| |
|---|
| *Specify the exact environment for which you will need access and plan to conduct testing activities* |

# Attachment C to Appendix 5
# Specification Sheet for a Data Service

Assumption

| |
|---|
| *List all assumptions for testing activities* |

Test Cases

| Case # | Scenario | Type of Test | Expected Result |
|---|---|---|---|
| *1 to N* | *Describe the test case including input data values* | *Positive, Negative, Stress, Endurance* | *Describe the expected results* |
| | | | |
| | | | |
| | | | |

# Attachment D to Appendix 5
# User Confidentiality Agreement Acknowledgement Form

**ACKNOWLEDGEMENT FORM _____of _____**

INDIVIDUAL'S FULL
NAME:_____

JOB TITLE AND LOCATION:

_____

EMPLOYER'S NAME:

_____

IF EMPLOYER IS NOT [RECIPIENT], PLEASE EXPLAIN:

_____

REASON(S) FOR INDIVIDUAL'S ACCESS TO DATA:

_____

I _____ acknowledge that all Data received through the statewide E-MOU is confidential and must be protected from unauthorized disclosure and use. I have been provided access to a copy of the Data Sharing Agreement (whether on paper or electronically) and agree to abide by the same restrictions and conditions that apply to Data User with respect to the Data as stated in Article IV. I have been instructed by the Partner on the permissible use(s) of the Data and will not use the Data for any other purpose. Partner has provided me with a list of the individuals with whom I may share the Data. I understand that I may not share the Data with any other entity or person, including but not limited to other employees, agents, or contractors of Partner who are not authorized to access the Data. I have received instructions from Partner on the proper way to store, handle, and protect the confidentiality of the Data and shall take all necessary steps to reduce the risk of unauthorized disclosure of use. I understand that I must report all violations of this agreement to the E-MOU Operational Committee per Article VI. Finally, I understand that unauthorized use of disclosure of the Data to any unauthorized individual or entity, is punishable by State and Federal statutes that impose legal sanctions.

**INDIVIDUAL**

Signature:_____

Date:_____

**FOR RECIPIENT:**

# Attachment D to Appendix 5
# User Confidentiality Agreement Acknowledgement Form

Name:_____

Title:_____

Signature:_____

Date_____