Fairfax County
Enterprise Memorandum
Of Understanding (E-MOU)

Version Date: November 4, 2021

List of Appendices and Attachments

Enterprise Memorandum of Understanding (E-MOU)

WHEREAS, certain Fairfax County agencies and entities (the "Participating Agencies") are seeking to integrate County data for proper purposes as outlined in the Government Data Collection and Dissemination Practices Act ("GDCDPA"). This E-MOU outlines the policies and procedures by which Participating Agencies may consent to Data Transmittals with other Participating Agencies, whether identifiable Data is transmitted, whether anonymized Data is transmitted, or whether Data is transmitted by Secure Data Environment.

The GDCDPA authorizes the sharing of information from agency systems for the following purposes:

> (i) to streamline administrative processes to improve the efficiency and efficacy of services, access to services, eligibility determinations for services, and service delivery; (ii) to reduce paperwork and administrative burdens on applicants for and recipients of public services; (iii) to improve the efficiency and efficacy of the management of public programs; (iv) to prevent fraud and improve auditing capabilities; (v) to conduct outcomes-related research; (vi) to develop quantifiable data to aid in policy development and decision making to promote the most efficient and effective use of resources; and (vii) to perform data analytics regarding any of these purposes.

Va. Code § 2.2-3801. The Participating Agencies include any Fairfax County agencies who are signatories to this E-MOU.."), Partners include: the Department of Information Technology ("DIT"), the Department of Management and Budget ("DMB"), the Office of the County Attorney ("OCA"), the Office of the County Executive ("CEX"), and the Internal Audit Office ("IAO").

WHEREAS, the Participating Agencies desire to securely exchange data as permitted or required by applicable law to increase the efficiency and effectiveness of programs they operate for the benefit of the residents of Fairfax County;

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, Participating Agencies; rather, the Participating Agencies enter into this E-MOU to enable their participation in the Data Exchange Service, as defined and set forth below;

WHEREAS, once the Participating Agencies enter into this E-MOU, they hope that other governmental entities will participate in the Data Exchange Service in the future, and each new entity shall be known as a "Participating Agency" provided that they execute and join this E-MOU;

WHEREAS, any Data Requests from and Data Transmittals to third parties (that are not signatories to this E-MOU) shall require execution of a separate Data Sharing or Data Use Agreement;

NOW, THEREFORE, for and in consideration of the mutual covenants contained herein, the Participating Agencies 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 among the Participating Agencies. 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 County 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** means all applicable federal, state, and local laws, regulations, and policies. Any references to Applicable Law or standards, including NIST, reference the most current version of such law or standard.

b. **Anonymize** means to deidentify Data by removing Personally Identifiable Information, such that it cannot be reidentified or otherwise used to identify an individual, in accordance with Applicable Law. Protected health information and substance use disorder information must be deidentified in compliance with HIPAA, 45 CFR § 164.514(b).

c. **Authorization** means that an Individual consents to the use or disclosure of Data pursuant to the requirements set forth at 45 CFR § 164.508 and any similar Applicable Laws, including 42 CFR § 2.31 and Va. Code § 32.1-127.1:03(G). 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 Participating Agency providing the data.

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

e. **Changes** means Development Changes (as used in Appendix 6 and defined in Appendix 6, Section 1.A) and Compliance Changes (as used in Appendix 6 and defined in Appendix 6, Section 1.B). Changes will be managed in accordance with Appendix 6 of this E-MOU.

f. **Coordinating Committee** is the governance body comprised of appointees from the Participating Agencies and Partners. The Coordinating Committee oversees and manages the requirements and processes outlined in this E-MOU.

g. **Data** means 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 Participating Agency to another Participating Agency under this Agreement. Data disclosed by a Participating Agency will be considered a copy that Discloser's Data. The Discloser will remain the custodian of that Data for

purposes of a Freedom of Information Act Request, subpoena, court order or other third party request related to the Data.

h. **Data Exchange Service** means hardware, software programs, protocols, and other such technological features and tools that serves to securely and safely share Data between Participating Agencies. Requirements for Data Exchange Services are defined in Appendix 8 of this E-MOU.

i. **Data Request** means a request for Data made by one Participating Agency to another and defined by an approved E-MOU Specification.

j. **Data Transmittal** means an electronic exchange of Data between Participating Agencies using agreed upon Specifications.

k. **Digital Credentials** means a mechanism, such as a public-key infrastructure, that enables Participating Agencies to electronically prove their identity and their authority to conduct data transmittal with other Participating Agencies. Any such mechanism must include two-factor authentication.

l. **Digital Signatures** are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. Digital Signatures must meet current industry standards and NIST Guidelines (NIST FIPS 186).

m. **Discloser** means a Participating Agency that discloses Data to another Participating Agency through a transmittal in any format.

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

o. **Effective Date** means the date of execution of this E-MOU by two or more Participating Agencies.

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

q. **Executive Committee** is the appeals and oversight body comprised of the County's Data Analytics Governance Council, or their designees.

r. **Individual** means a client or person whose data is maintained by a Participating Agency and subject to exchange with participating agencies.

s. **Information Technology Service Provider or ITSP** means the Fairfax County Department of Information Technology or other organization that will support one or more Participating Agencies by providing them with operational, technical, cloud, or information technology services.

t. **Notice or Notification** means a written communication sent to the appropriate

Participating Agency's representative in accordance with the other policies and procedures attached to this E-MOU.

u. **Operational Measures or Operational Data** means 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 will not contain any individually identifiable data or protected content.

v. **Participating Agency** means any "agency" as defined in Va. Code § 2.2-3801, or other entity that is a signatory to this E-MOU

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

x. **Partner** means any "agency" as defined by Va. Code § 2.2-3801 or other entity that is a necessary signatory to this E-MOU and that contributes services or other support to Participating Agencies or that may be a beneficiary to data-sharing as authorized by this E-MOU. Partner also means any ITSP working specifically for a Participating Agency. Partners are bound by the same requirements as Participating Agencies if Requesting, Transmitting, or Receiving Data under this E-MOU.

y. **Personally Identifiable Information (PII)** is information that can be used to distinguish or trace an individual's identity, such as, for example, their name, social security number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

z. **Production Data** means Data created by a Participating Agency in accordance with the Validation Plan and used by the Participating Agency 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.

aa. **Recipient** means the Participating Agencies, users, vendors, and any other person or entity that receives or has access to the Data through a Data Transmittal from a Discloser pursuant to this E-MOU.

bb. **Secure Data Environment** (SDE) is a transaction processing environment, built upon web services architecture, supporting the capabilities to assure security of access and protections of privacy for the individuals served. The SDE does not store data except transaction activity, including user identifications, stored for auditability of data uses. All data exchanges, including response to inquiry translations, as well as the links to those data are dynamic, and only last for the duration of the transaction.

cc. **Specifications of Service or Service Specification or Specifications** means the specifications established by Applicable Law and adopted by the Coordinating Committee that prescribe the Data content, technical, and security requirements needed to enable the Participating Agencies 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 8, and may be amended in accordance with Appendices 6 and 9.

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

ee. **Test Data** means Data created by a Participating Agency in accordance with the Validation Plan and used by the Participating Agency 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 Participating Agencies. In the case of such exceptions, all production level data security protocols must be adhered to.

ff. **Testing** means the tests and demonstrations of a Participating Agency's System and processes used for interoperable Data Transmittal to assess conformity with the Emergent Specifications, Specifications and Validation Plan.

gg. **Transmit, Transmittal or Transmitting** means, in varying tenses, to send Data electronically using the Specifications.

hh. **User** means any employee of a Participating Agency or individual or entity who has been authorized to access the Data through the respective Participating Agency's System in accordance with Applicable Law and this E-MOU.

ii. **Validation Plan** means the framework for Testing and demonstrations for Participating Agency seeking to use a Data Exchange Service. The Validation Plan is attached hereto as part of Appendix 9, and must be in compliance with Appendix 6 and Appendix 8.

ARTICLE III
RESPONSIBILITIES OF THE COORDINATING COMMITTEE

The Partner Agencies will work in cooperation with the Participating Agencies to create a Coordinating Committee to support secure Data Transmittal and develop the Specifications, including Emergent Specifications, with which the Participating Agencies will comply with Data Transmittal. The Coordinating Committee will be comprised of a designee from each Partner Agency and each Participating Agency, except that DIT will designate two members, one from the Information Security Office and one from another office within DIT. The County's HIPAA Compliance Officer, or their designee, will also be a member. The Chairperson of the Committee will be a member of the County Executive's Office, or another County Executive designee. Each member of the Coordinating Committee will have one vote. OCA will designate an individual to attend Coordinating Committee meetings as needed; however, OCA will not have a vote on the Committee.

The Coordinating Committee will meet quarterly unless meetings on specific issues are required as outlined in this E-MOU. One week prior to a scheduled meeting, the Chairperson will send the Coordinating Committee the agenda for the meeting. If specific members are needed to accomplish the tasks outlined on the agenda, the Chairperson will specifically request the presence of those members. The majority vote of those present at the Coordinating Committee meeting is binding.

Members may participate and vote electronically. The Participating Agencies agree to designate support staff from their own organizations as required to provide a sufficient degree of support needed to carry out the activities of the Coordinating Committee as described below.

The Coordinating Committee will conduct the following activities regarding specific Data Exchange Service:

a. Maintain a list of all E-MOU Participating Agencies, their designated representative(s) and their preferred contact information where they can be reached, which shall be available to all E-MOU Participating Agencies as needed;

b. Assist with the resolution of Disputes between Participating Agencies in accordance with this E-MOU;

c. Manage the amendment of this E-MOU in accordance with Appendix 5 of this E-MOU;

d. Receive reports of Breaches, notify Participating Agencies of Breaches, receive confirmation from Participating Agencies when the security of their Systems have been restored after Breaches, and notify Participating Agencies when all issues leading to a Breach have been resolved. Notification of a Breach to the Coordinating Committee does not relieve the Participating Agency 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;

e. Determining when to issue a finding or suspend data exchanges accordance with Appendix 4 of this E-MOU;

f. Develop, evaluate, prioritize, and adopt Specifications, including Emergent Specifications, changes to such Specifications, and the artifacts required by the Validation Plan in accordance with Appendix 8 and Appendix 9 of this E-MOU. Any Specifications developed will comply with Applicable Law;

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

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

i. Perform impartial review of Participating Agencies' compliance with the Specifications as defined in Appendix 8 of this E-MOU;

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. Audit the environment of any Participating Agency-specific IT system that will be receiving data through this E-MOU;

l. Create and maintain a record of any disclosure of Data made to other persons or

entities not having regular access to Data. The record of disclosure will 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; and

m. Convene subject area-specific task groups or subcommittees as needed.

ARTICLE IV
USE OF DATA

a. **Permitted Purpose.** Participating Agencies will only Request and Transmit Data in accordance with Applicable Law, including proper purposes under the GDCDPA (Va. Code § 2.2-3801), the HIPAA Privacy and Security Rules (45 CFR Part 164), and the regulations governing the Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2), as applicable. Participating Agencies will ensure adequate training of Applicable Law and enforce such requirements 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 will only retain and use Data in accordance with (i) Applicable Law, (ii) the purposes for which the Data was made available under the Business Purposes provided in the Specifications Sheet as described in Appendix 8; (iii) and the Recipient's record retention policies and procedures. Recipients will not disclose Data to any outside entity or person, including subcontractors, without the written permission of the Discloser.

c. **Management Uses.** The Coordinating Committee, or designee, may request operational measures from Participating Agencies regarding use of exchanged data, and Participating Agencies agree to provide requested measures in accordance with Applicable Law, for the purposes listed in Article VIII:, *Expectations, Duties, and Responsibilities of the Participating Agencies*.

d. **Authorization**. The Participating Agency certifies that unless permitted or required to share Data by Applicable Law, it has obtained a Uniform Authorization to Exchange Information from an Individual served by the Participating Agency for whom an inquiry is made, that permits the Participating Agency to disclose Data pursuant to this E-MOU. If the Participating Agency 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, upon verification of such authorization. No disclosure of any identifiable Data is permitted without such authorization from the Individual, unless such disclosure is permitted by Applicable Law.

e. **Tracking of Authorizations**. The Participating Agency agrees to track the expiration and/or revocation of Authorizations in compliance with Applicable Law, and specifically:

1) Defective authorizations. 45 CFR § 164.508(b)(2) and 42 CFR § 2.31(a)(6). 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 material information in an authorization is known by the covered entity to be false.

2) Revocations of authorizations 45 CFR § 164.508(b)(5) and 42 CFR § 2.31(a)(6) -. An Individual may revoke an authorization at any time, 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 Participating Agency agrees to have Participating Agency Access and Disclosure Policies. Each Participating Agency acknowledges that Participating Agency Access and Disclosure Policies may differ among them as a result of differing Applicable Law and business practices. Each Participating Agency agrees to be responsible for encrypting data in transit and at rest using NIST SP 800-57 or current industry standard algorithms agreed on by the Participating Agencies involved before transmission occurs based on the application of its Participating Agency Access and Disclosure Policies to the requested Data. Each Participating Agency shall comply with Applicable Law, this E-MOU, and all applicable Specifications in Transmittal of Data.

b. **Authentication.** Each Participating Agency agrees to use an approved credentialing tool through which the Participating Agency, or its designee, uses Digital Credentials to verify the identity of each User prior to enabling such User to Transmit Data. The 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 Participating Agency agrees to proceed according to applicable guidance contained in (FISM) NIST SP800-39, Managing Information Risk, and County Procedural Memorandum Participating Agency will be responsible for maintaining a secure environment compliant with State policies, standards and guidelines, and other Applicable Law that supports the Transmission of Data 70-05, found at DIT's Information Security Intranet site. Furthermore, each in compliance with the Specifications. Participating Agencies will use appropriate safeguards to prevent use or disclosure of Data other than as permitted by this E-MOU and Applicable Law, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Data. Appropriate safeguards will 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 Coordinating Committee or designee or the DIT Information Security Office 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 Participating Agencies involved before transmission occurs. Each Participating Agency agrees to, as appropriate under Applicable Law, have written privacy and security policies, including Access and Disclosure Policies, in place before the Participating Agency'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, Participating Agencies will comply with any Specifications that define expectations with respect to enterprise security.

b. **Malicious Software.** Each Participating Agency 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 (i) a System, or any part thereof, or (ii) any hardware or software used by a Participating Agency in connection therewith, or (iii) 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 Participating Agency in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. Participating Agency agrees to meet the applicable guidance 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 Participating Agency on its side of the exchange will 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 Participating Agency shall ensure that it is meeting the applicable guidance 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 Participating Agency 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 Participating Agency will comply with FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems. Participating Agencies will ensure that System solutions that store, transmit, receive, and permit access are compliant with the Specifications and with the applicable guidance contained in (FISM) NIST 800-60, Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories.

d. Each Participating Agency will, 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 Participating Agency will develop auditing activities reflecting the guidance in (FISM) NST SP800-137, Information Security Continuous Monitoring (ISCM) and will 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 (NIST SP 800-52). Digital signatures should be used in transmissions to identify the source and destination.

f. **Exception Process**. A Participating Agency that does not yet fully meet the requirements set forth above in Article VI may apply to the Coordinating Committee with a proposed plan to share data during the process of coming into full compliance with the stated requirements.

ARTICLE VII
SPECIFICATIONS

a. **General Compliance.** Each Participating Agency shall comply with all of the Specifications under this E-MOU, and identified hereto as Appendix 7, unless compliance would be a violation of Applicable Law.

b. **Adoption of Specifications.** The Participating Agencies hereby acknowledge the role of the Coordinating Committee as the mechanism whereby the Participating Agencies can jointly advise the adoption of Service Specifications and Emergent Specifications, and that the Coordinating Committee may recommend the adoption of amendments to, or repeal and replacement of, the Service Specifications at any time, as outlined in Appendix 5 and Appendix 7 of this E-MOU.

c. **Specification Amendment Process.** The Specifications will be amended as set forth in Appendix 5 of this E-MOU.

ARTICLE VIII
EXPECTATIONS, DUTIES, AND RESPONSIBILITIES OF PARTICIPATING AGENCIES

a. **Minimum Requirements for Participating Agencies Regarding Data Requests.** All Participating Agencies that make Data Requests, or allow their respective Users to make Data Requests, shall have a collaborative relationship and respond to Data Requests when made to them by another Participating Agency in the affirmative, unless specifically prohibited by Applicable Law. If the request cannot be fulfilled, the Participating Agency will provide the legal authority on why the request cannot be complied with and how to overcome the prohibition. Data Requests can be made directly to a Participating Agency, or through the Secure Data Environment, as outlined in Appendices 1, 2, and 3. Participating Agencies must be approved to request Data from the specified Data Exchange Service as defined in Appendix 7 and 8. Nothing in this E-MOU requires a Data Transmittal that would violate Applicable Law. However, if the transmission of the Data to Participating Agencies is specifically prohibited by state or federal law, Participating Agencies will work to identify if any edits, deletions or additional protections can be made to allow the Data to be provided to a Participating Agency.

b. **Users and Information Technology Service Provider (ITSPs).** Each Participating Agency will 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. **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 will be maintained and who has access to the Data), each Participating Agency must comply with Applicable Law, applicable Participating Agency Access and Disclosure Policies, the Specifications, this enterprise standard and this E-MOU, and will meet all of the requirements set forth by the DIT Information Security Office in conformity with (FISM) NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

2. Safeguards**.** Participating Agencies shall use reasonable and appropriate

administrative, physical and technical safeguards as defined by the DIT Information Security Office in conformity with (FISM) SP800-47, Security Guide for Interconnecting Information Technology Systems, and comply with the Specifications to protect Data and to prevent its unauthorized disclosure.

3. Breach Notification**.** Participating Agencies will report to the Coordinating Committee all Breaches that threaten the security of the databases and Data communications resulting in exposure of Data, or other incidents compromising the security of the information technology systems with the potential to cause major disruption to normal agency activities in accordance with Appendix 7 of this E-MOU. Such reports must be made to the Coordinating Committee or designee immediately when the Participating Agency discovered or within 24 hours from when the Participating Agency should have discovered the occurrence. Participating Agencies must also comply with any Applicable Law regarding data breaches.

4. Conflict of Obligations. This Article does not supersede a Participating Agency's obligations (if any) under relevant security incident, breach notification, or confidentiality provisions of Applicable Law.

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

d. **Responsibilities of the Participating Agencies.** Each Participating Agency hereby agrees to the following:

1. Data Requested by the Coordinating Committee. Each Participating Agency will provide the Coordinating Committee with all Operational Measures reasonably requested by the Coordinating Committee to discharge its duties under this E-MOU or Applicable Law. Any Operational Measures provided by a Participating Agency to the Coordinating Committee shall be responsive and accurate. Each Participating Agency agrees to provide Notice to the Coordinating Committee if any Operational Measures provided by the Participating Agency materially changes. Each Participating Agency agrees to cooperate in the confirmation or other verification of the completeness and accuracy of any Operational Measures provided. At any time, each Participating Agency agrees to cooperate with the Coordinating Committee in such requests, given reasonable prior Notice. The goal is for the Participating Agency to respond to a request within one business day; if the Participating Agency cannot respond within one business day, the Participating Agency must request additional time to respond and such reasonable requests will be granted. If a Participating Agency cannot in good faith provide Operational Measures as requested by the Coordinating Committee, the Participating Agency may ask for relief from the request in writing to the Coordinating Committee.

2. Execution of the E-MOU. Each Participating Agency shall execute this E-MOU and return an executed copy to the Coordinating Committee. In doing so, the Participating Agency affirms that it has full power and authority to enter into and perform this E-MOU. The Participating Agency Director shall be the representative authorized to sign on behalf of the Participating Agency. The Participating Agency Director or designee will maintain the E-MOU documents and make it accessible to all Participating Agencies and members of the Coordinating Committee.

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

4. Agreements with Users. Each Participating Agency will have established agreements with each of its Users that require the User to, at a minimum:

(i) Comply with all Applicable Law;
(ii) Train Users on Applicable Law and requirements related to this E-MOU;
(iii) Reasonably cooperate with the Participating Agency on issues related to this E-MOU;
(iv) Transmit Data only for a permitted purpose;
(v) Use and disclose Data received from another Participating Agency or User only in accordance with the terms and conditions of this E-MOU;
(vi) Immediately upon determining that a Breach occurred, User will report such Breach to the Coordinating Committee, as well as follow its agency's internal reporting procedures;
(vii) Refrain from disclosing to any other person any passwords or other security measures issued to the User by the Participating Agency;
(viii) Sign the User Acknowledgement form found in Appendix 8, Attachment A; and
(ix) Cooperate with any external audits.

Notwithstanding the foregoing, for Users who are employed by a Participating Agency or who have agreements with the Participating Agency that 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 Participating Agency 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 Participating Agency uses vendors in connection with the Participating Agency's Transmittal of Data, each Participating Agency 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, including, but not limited to, executing the Fairfax County Business Associate Agreement or Qualified Service Organization Agreement as appropriate (https://www.fairfaxcounty.gov/topics/hipaa-business-associate-agreements);
(ii) Protect the privacy and security of any Data to which it has access;
(iii) After determining that a Breach occurred, immediately report such Breach to the Participating Agency;
(iv) Not to re-disclose information without consent of the Participating Agency;
(v) Use information only for the purposes for which it was made available under the Business Purposes provided in the Specifications Sheet;
(vi) Agree to the same restrictions on the access, use, and disclosure of Data as contained herein;
(vii) Reasonably cooperate with the other Participating Agencies to this E-MOU on issues related to this E-MOU;
(viii) Sign the User Acknowledgement form found in Appendix 8, Appendix D; and
(ix) Cooperate with any external audits.

6. Creation of Test Data. Certain Participating Agencies may agree to create Test Data (non-Individual/hypothetical data created for testing purposes only) to be used by other Participating Agencies for testing. Any Test Data shall not be generated or synthesized from Production Data and 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 Participating Agency 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 Participating Agency 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**.** User shall notify the Coordinating Committee and the original Discloser Agency immediately when User receives a Freedom of Information Act Request ("VFOIA"), subpoena, court order or other third party request related to the Data. The Coordinating Committee, in conjunction with the Disclosure Agency, shall determine whether the information sought contains identifiable or confidential information and whether it shall be released. User shall refer all such communications to the Coordinating Committee and original Discloser Agency for their joint response, which response shall comport with all statutory and judicial deadlines, as applicable. Nothing in this section shall require User to not comply with a valid court order.

e. **Treatment of Data**. Each Recipient and User 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 and Users 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 8. See Appendix 8, Attachment A.

f. **Disclaimers.**

1. Reliance on a System. Each Participating Agency 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 Participating Agency related to the clinical accuracy, content, or completeness of any Data provided pursuant to this E-MOU. The Participating Agencies acknowledge that other Participating Agencies' Digital Credentials may be activated or suspended at any time; therefore, Participating Agencies may not rely upon the availability of a particular Participating Agency's Data.

2. Carrier lines. All Participating Agencies acknowledge that the Transmittal of Data between Participating Agencies 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 Participating Agencies' control. Provided a Participating Agency 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 Participating Agencies 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 Participating Agencies' 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 Participating Agencies' control. Use of the carrier lines is solely at the Participating Agencies' 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 Participating Agency responsible for the Data being transmitted is the responsible party for the Breach Notification. However, data should be encrypted using NIST FIPS 197 or 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 beginning 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 Coordinating Committee by providing to Participating Agencies 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 4, Section 1 of this E-MOU.

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

d. **Effect of Termination of Data Exchange Project.** Upon termination or suspension 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 guidance for "Purge" contained in NIST SP800-88, Appendix A: Minimum Sanitization Recommendation for Media Containing Data." DIT shall verify that Recipient properly purged the Data.

e. **Dispute Resolution Process.**

1. General. If any Dispute arises between Participating Agencies regarding the implementation of this E-MOU, those Participating Agencies agree to commence efforts to resolve such Dispute in good faith, and if the Dispute cannot be resolved, then the Participating Agencies may seek the involvement of a designated subcommittee of the Coordinating Committee. The subcommittee will be formed by the Coordinating Committee within seven (7) business days after written notification of any such Dispute that could not be otherwise resolved. Any Participating Agency may submit written notification of such a Dispute to the Coordinating Committee. The subcommittee shall endeavor to resolve the Dispute, but if the Dispute cannot be resolved, then the Dispute will be addressed by the entirety of the Coordinating Committee, which will render its decision with within ten (10) business days of written notice by the chair of the designated subcommittee that the Dispute could not be resolved.

2. Activities during Dispute Resolution Process. Pending resolution of any

Dispute under this E-MOU, the Participating Agencies agree to fulfill their responsibilities in accordance with this E-MOU, unless the Participating Agency is suspended by the Coordinating Committee pursuant to the procedures outlined in Appendix 4.

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

4. Disputes between a Participating Agency and the Coordinating Committee. If any Dispute arises between a Participating Agency and the Coordinating Committee, such Disputed Matter is escalated to the Executive Committee for resolution. If the Disputed Matters is not resolved by the Executive Committee, the Matter is escalated to the County Executive for final resolution.

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

ARTICLE X
MISCELLANEOUS

a. **Notices.** All Notices to be made under this E-MOU shall be given in writing to the authorized Participating Agency's representative at the address listed with the Coordinating Committee, and shall be deemed given: (i) upon delivery, if personally delivered or through the 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 Coordinating Committee, and the recipient of such e-mail acknowledges receipt.

b. **Governing Law.** This E-MOU shall be governed by and construed in accordance with the applicable laws of the United States and the Commonwealth of Virginia, without regard to any conflict of laws principles that would result in the application of laws of any jurisdiction other than those of the United States or Virginia.

c. **Amendment.** An amendment of the E-MOU may be recommended by agreement of at least two-thirds of the Coordinating Committee. All Participating Agencies agree to sign an amendment adopted in accordance with the provisions of this Section in accordance with Appendix 4. Participating Agencies shall have the right to challenge an Coordinating 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 4 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 Coordinating Committee or designee. The Coordinating Committee or designee shall maintain the E-MOU is a format that is accessible to all E-MOU Participating Agencies.

e. **Validity of Provisions.** If 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.** If 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 captions of this Agreement are for reference only and do not describe the intent of this Agreement or otherwise alter the terms of this Agreement.

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

i. **Effective Date.** With respect to the first two Participating Agencies to this E-MOU, the Effective Date shall be the date on which the second Participating Agency executes this E-MOU. For all Participating Agencies thereafter, the Effective Date shall be the date that the Participating Agency 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 Participating Agency 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 Participating Agency 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 Coordinating Committee and the affected Participating Agency(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**. If any Data is required to be disclosed in response to a valid court order 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 Participating Agency will be

notified of the order and provided with a copy of such order upon its receipt, and Participating Agency may seek a protective order.

p. **Public Access**. Unless subject to a specific statutory exemption, this E-MOU and its attachments are subject to disclosure under VFOIA. Any Data that is provided under this E-MOU will remain subject to any exemptions available when the Data was held by the Discloser, according to Applicable Law. A Recipient shall promptly notify a Discloser of any VFOIA request received by a Recipient for a Discloser's Data.

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

FAIRFAX COUNTY OFFICE OF THE COUNTY EXECUTIVE

By: Bryan Hill, County Executive

_____ _____

Signature Date

FAIRFAX COUNTY DEPARTMENT OF INFORMATION TECHNOLOGY

By: Gregory Scott, Director

_____ _____

Signature Date

FAIRFAX COUNTY INTERNAL AUDIT OFFICE

By: Sharon Pribadi, Director

_____ _____

Signature Date

FAIRFAX COUNTY DEPARTMENT OF MANAGEMENT AND BUDGET

By: Christina Jackson, Director

_____ _____

Signature Date

FAIRFAX COUNTY OFFICE OF THE COUNTY ATTORNEY

By: Elizabeth Teare, County Attorney

_____ _____

Signature Date

_____ By: _____
Agency Director

_____ _____
Signature Date

_____ By: _____
Agency Director

_____ _____
Signature Date

_____ By: _____
Agency Director

_____ _____
Signature Date

_____ By: _____
Agency Director

_____ _____
Signature Date

_____ By: _____
Agency Director

_____ _____
Signature Date

_____ By: _____
Agency Director

_____ _____
Signature Date

Fairfax County
Enterprise Memorandum of Understanding (E-MOU)

Appendices

DATED: _____, 2021

Appendix 1
Identifiable Data Transmittals

When Data is transmitted from one Participating Agency to another, data-sharing will be governed by this Appendix and Appendices 4 – 8.

A. Data Transmittal from One Participating Agency to Another

a. A Disclosing Participating Agency will respond to Data Requests from a Receiving Participating Agency within ten business days. Such a response may be either (i) providing the requested Data, or (ii) advising the Participating Agency in writing why the Data is not available or cannot be lawfully exchanged. Any such written response must specifically state the legal authority regarding why the Data cannot be provided, and if possible, direction on how the Data may be lawfully exchanged. Data Transmittals in response to Data Requests will comply with the Specifications, this E-MOU, applicable Participating Agency Access and Disclosure Policies, any applicable agreements between Participating Agencies and their Users, and Applicable Law.

b. As appropriate depending on the nature of the request, the Discloser will submit the requested Data to DIT or directly to the Recipient, or otherwise permit DIT staff to electronically access the requested Data in accordance with this E-MOU. Data will be transferred electronically only via encrypted files and in accordance with DIT's data security standards and policies, as outlined in this E-MOU.

B. Requirements for Use and Maintenance of Data

a. Data shall only be used and disclosed as authorized by this E-MOU and Applicable Law.

b. Recipient shall use appropriate safeguards to prevent use or disclosure of Data other than as permitted by this E-MOU and Applicable Law.

Appendix 2
Data Transmittals for Anonymization

When Data is transmitted from a Participating Agency to access anonymized Data or anonymize Data for research, data analytics, and other proper purposes, data-sharing will be governed by this Appendix and Appendices 4 – 8.

A. Data Transmittal for accessing Anonymized Data or Anonymization

a. When a Participating Agency makes a Data Request for purposes of accessing Anonymized Data or Anonymizing the Data, the Disclosing Participating Agency will respond within ten business days. Such a response may be either (i) providing the requested Data, or (ii) advising in writing why the Data is not available or cannot be lawfully exchanged. Any such written response must specifically state the legal authority regarding why the Data cannot be provided, and if possible, direction on how the Data may be lawfully exchanged. Data Transmittals in response to Data Requests will comply with the Specifications, this E-MOU, applicable Participating Agency Access and Disclosure Policies, any applicable agreements between Participating Agencies and their Users, and Applicable Law.

b. As appropriate, depending on the nature of the request, the Discloser will submit the requested Data to DIT or directly to the Recipient, or otherwise permit DIT staff to electronically access the requested Data in accordance with this E-MOU. Data will be transferred electronically only via encrypted files and in accordance with DIT's data security standards and policies, as outlined in this EMOU. For Data Requests that require repeated Data Transmittals, the Parties shall agree upon the frequency of the Data Transmittals, reporting requirements, and specifications to maintain current Data in the appropriate Data Warehouse or other Repository.

c. If anonymization is required, DIT or other ITSP will Anonymize the Data in accordance with this E-MOU and Applicable Law prior to disseminating the Data to the Recipient. The ITSP may first match and integrate multiple sources of Data to create an Anonymized Data set.

B. Access to Anonymized Data and Dashboard Applications

a. DIT shall maintain an inventory of Disclosers' Data Transmittals to any Data Warehouse or other Repository and provide the inventory to Participating Agencies upon request. Updated inventory will be provided to DMB quarterly to support countywide Data Analytics efforts.

b. Disclosers and Recipients shall designate Users to have access to the Anonymized Data set. DIT shall provide such Users with timely access to the Anonymized Data or Dashboard Application, as appropriate, once Users have complied with Article VIII, Section D(4) of this E-MOU.

Appendix 2
Data Transmittals for Anonymization

C. Requirements for Use and Maintenance of Data

a. Both identifiable Data and Anonymized Data shall only be used and disclosed as authorized by this E-MOU and Applicable Law. Unless prohibited by Applicable Law, Data may be disclosed for proper purposes under the GDCDPA.

b. Recipient shall use appropriate safeguards to prevent use or disclosure of Data other than as permitted by this E-MOU and Applicable Law.

Appendix 3
Data Transmittal By Secure Data Environment

When data is transmitted through the Secure Data Environment, data-sharing will be governed by this Appendix and Appendices 4 – 8.

A. General Principles

a. No Participating Agency will access another Participating Agency's system. Instead, data will be placed outside the Participating Agency's home network, where all data will be available to answer queries by another Participating Agency.

b. All data made available to the SDE is at the discretion of each Participating Agency. Once data is determined to be sharable by the agency, a Metadata framework is developed. The Metadata framework identifies the data elements to be shared, in accordance with policy/legal conformance, as well as the translated values for each data element to be shared. The data element and responses selected are at the full discretion of the Discloser.

B. Process to Initiate Data Sharing

a. Each Participating Agency agrees to establish authentication for and to credential Users and will share such credentialing of Users with the SDE.

b. Prior to Participating Agencies making data elements available to share with other Agencies, executive, legal, and technology representatives shall review each data element and agree that the data element is available to share, whether it shall be made available, to whom, and under what circumstances.

c. Each Participating Agency shall make data elements available for access in accordance with the terms and conditions of the E-MOU, including without limitation those governing the authorization, use, confidentiality, privacy, and security of the Data Elements.

d. Access rules are set and controlled by the Discloser.

e. If Applicable Laws require an Authorization from the individual who is the subject of the Data element in order for the requesting Participating Agency to have access, the requesting Participating Agency shall ensure that there is a valid Authorization on file with the SDE.

C. Process of Data Exchanges

a. Users are provided their access credentials by their home agency.

b. Legal and regulatory requirements are built into the automated transaction processing environment. The SDE maintains the rules of access and use for each user.

Appendix 3, Continued
Data Transmittal By Secure Data Environment

c. Participating Agency Users will assert identity and access credentials when requests are made to enter the SDE. The SDE will validate the User's credentials and role-based access privileges/attributions. The process will inform the User if they are not authorized to access the data; otherwise the request will be processed.

d. The data will be encrypted and will only be available via internal SDE program interface.

D. Use of Data

a. Data shall only be used and disclosed as authorized by this E-MOU and Applicable Law.

b. Recipient shall use appropriate safeguards to prevent use or disclosure of Data other than as permitted by this E-MOU and Applicable Law.

E. Auditing of System

a. All SDE transaction activity will be logged and will include granular data on access, use, inquiries and data types inquired/responded; recordation of all transaction activity.

b. Each Participating Agency has the ability to monitor and audit all access to its data and information obtained through this E-MOU, to ensure system administration, security, and that access is strictly for legitimate purposes. Each Participating Agency shall have access to such auditing activities.

Appendix 4
Procedures for Adding a New Participating Agency and Suspending a Participating Agency

1. Adding a New Participating Agency

When an Applicant requests to join this E-MOU, the request shall be directed to the Chairperson of the Coordinating Committee in writing. As laid out in Appendix 8 Section 1, the Applicant must submit an E-MOU Data Services Request Form to inform the Coordinating Committee which Data Exchange Services it wants to access. If the Applicant's request is approved, the Applicant must submit an Internal Control Questionnaire ("ICQ") to the Coordinating Committee laying out details of how the Applicant intends to secure the data it will receive. Finally, if the Applicant's ICQ is approved, Applicant must submit a Specification Sheet listing a specific business reason why access is desired.

If no concerns are identified, the Applicant will be approved to begin new Participating Agency testing as defined by the On-boarding Validation Plan in Appendix 9 to be reviewed and amended, as necessary, by the Coordinating Committee of this E-MOU.

Once the Applicant has successfully completed the On-boarding Validation Plan as defined in Appendix 9, the Chairperson shall facilitate a review by the Coordinating Committee within ten business days of the User Acceptance Testing (UAT) Report for compliance with the Validation Plan.

Once the Coordinating Committee approves the Applicant's Test Report for UAT, the Applicant will be considered a Participating Agency and shall execute this E-MOU with its supporting appendices.

If the Coordinating Committee does not approve the Applicant's UAT Test Report, the Coordinating Committee will advise the Applicant with specific remediation guidance to improve compliance when re-testing. If the Applicant may appeal the denial of the UAT Test Report to the Director of DIT. If the matter is not resolved by DIT, then the matter shall be escalated to the Executive Committee for final resolution.

2. Suspension

A. Voluntarily by the Participating Agency

1. Service Level Interruptions

Participating Agencies 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 Participating Agency having to temporarily cease Data Transmittals with other Participating Agencies. To ensure that all Participating Agencies are aware of service level interruptions, the Participating Agency experiencing the service level interruption agrees to notify

the Coordinating Committee or its designee of the interruption prior to the interruption, if planned, or as soon as reasonably practicable after the interruption begins, if unplanned. The Coordinating Committee or its designee shall simultaneously notify all other Participating Agencies of the interruption. Since a service level interruption does not involve the suspension of a Participating Agency's Digital Credentials, the Participating Agency agrees to be responsible for taking all technical actions necessary to resolve a service level interruption. During a service level interruption, the Participating Agency agrees to continue to comply with the terms and conditions of the E-MOU.

2. Voluntary Suspension

If a Participating Agency decides that it requires a temporary suspension of its Digital Credentials and its responsibility for complying with the terms of the E-MOU, it agrees to provide Notice to the Coordinating Committee of its need for a temporary voluntary suspension at least twenty-four 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 Coordinating Committee or its designee shall simultaneously notify all other Participating Agencies of the voluntary suspension.

B. With Cause

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

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

If the Coordinating Committee determines that the Participating Agency does not substantially cure its material default within thirty days following receipt of the written Notice of such default from the Coordinating Committee, the Coordinating Committee may suspend the Participating Agency. Upon suspension, Disclosers may request that any Data held by the Participating Agency be transferred or purged in accordance with Section IX(d) of this E-MOU.

Additionally, upon receipt by the Coordinating Committee of a complaint, report, or other information (complaint) about a Participating Agency questioning whether a Participating Agency's information technology (IT) System is creating an immediate threat of Data Breach or will cause irreparable harm to another Participating Agency, the Coordinating Committee shall

have the ability to investigate the complaint, and determine whether to issue a finding requiring a Corrective Action Plan to remedy the issue for the specific IT System.

When the complaint indicates that a suspension from receiving data to a Participating Agency's specific IT system must be implemented immediately and, in the judgment of the Chairperson, it is not practical to delay the suspension while the Coordinating 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 Participating Agency's Digital Credentials to receive, but not provide, data to E-MOU Participating Agencies from the IT system in question;
- call a special meeting of the Coordinating Committee to evaluate the recommendation of suspension; and
- notify the suspended Participating Agency of the suspension.

If the Chairperson determines that immediate suspension is not required, the Coordinating Committee may initiate an investigation of the complaint. The Coordinating Committee Chairperson shall immediately notify the Participating Agency in question of the investigation.

In the event of an immediate suspension by the Chairperson, the Coordinating Committee shall meet as soon as practicable, but no later than five business days after the suspension. The suspension shall remain in effect until the Coordinating Committee meets to evaluate the suspension and determines whether to affirm, modify, or terminate the suspension.

If a complaint is referred to the Chairperson and such complaint has not been resolved by the Coordinating Committee within thirty (30) days after it was first referred to the Chairperson (or such longer period as agreed to in writing by the Participating Agencies who are the subject of the complaint), then the complaint shall be escalated to the Executive Committee for resolution. If the complaint is not resolved by the Executive Committee within five business days from the referral, then the complaint is dismissed with no action taken against the Participating Agency.

If, through the investigation, the Coordinating Committee recommends that a Participating Agency is (i) creating an immediate threat or (ii) will cause irreparable harm to another party, including, but not limited to, another Participating Agency, a User, the Coordinating Committee, or an individual whose Data are exchanged pursuant to the E-MOU, the Coordinating Committee may recommend that such Participating Agency be issued a finding requiring a Corrective Action Plan to remedy the issue for the IT system. The Coordinating Committee may take all technical actions necessary to carry out the finding or suspension including, but not limited to, suspension of the Participating Agency's Digital Credentials to receive data from, but not provide data to E-MOU Participating Agencies from the IT system in question. As soon as reasonably practicable after suspending a Participating Agency, but in no case longer than three business days, the Coordinating

Appendix 4, Continued
Procedures for Adding a New Participating Agency and Suspending a Participating Agency

Committee Chairperson shall provide the suspended Participating Agency with a written summary of the reasons for the suspension and notify all other Participating Agencies of the suspension.

Upon suspension, Disclosers may request that any Data held by the Participating Agency be transferred or purged in accordance with Section IX(d) of this E-MOU.

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

Any objection shall specify the reason that the Participating Agency feels the suspension is inappropriate. The plan of correction shall describe the action that the Participating Agency is taking to address, mitigate and remediate the issue(s) that caused the Coordinating Committee to recommend that a suspension was appropriate and include a timeframe for such actions. The Coordinating Committee shall meet and review a suspended Participating Agency's plan of correction or objection within five business days of receipt from the Participating Agency; determine whether to recommend to accept or reject the plan of correction or affirm the suspension; and communicate such decision to the suspended Participating Agency.

If the Coordinating Committee rejects the plan of correction, it shall work in good faith with the suspended Participating Agency to develop a mutually acceptable plan of correction. If the Coordinating Committee and the suspended Participating Agency cannot reach agreement on the content of the plan of correction or on the reasons supporting the suspension, the Coordinating Committee may submit the Dispute to the Executive Committee for resolution. If the Dispute is not resolved by the Executive Committee, the Matter is escalated to the County Executive for final resolution.

Any suspensions imposed shall remain in effect until the Participating Agency is reinstated.

A finding requiring a Corrective Action Plan, but not a suspension, shall describe the action that the Participating Agency is taking to address, mitigate and remediate the issue(s) that caused the Coordinating Committee to make the finding and include a timeframe for such actions. The Participating Agency's Corrective Action Plan in response to a Coordinating Committee finding shall be submitted within thirty days of the finding being issues. The Coordinating Committee shall meet and review a Participating Agency's Corrective Action Plan at the next regular meeting following the submission of the Corrective Action Plan from the Participating Agency; determine whether to accept or reject the plan; and communicate such decision to the Participating Agency.

3. Reinstatement

A. After Voluntary Suspension by a Participating Agency

Appendix 4, Continued
Procedures for Adding a New Participating Agency and Suspending a Participating Agency

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

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

B. After Suspension with Cause

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

If the Coordinating Committee is not satisfied that the Participating Agency has met its obligations under its plan of correction, the Coordinating Committee Chairperson shall inform the Participating Agency of the deficiencies. The Participating Agency will have the ability to submit additional evidence that addresses such deficiencies

When the Coordinating Committee is satisfied that the evidence presented indicates that the Participating Agency has fulfilled its obligations under the Corrective Action Plan, it shall take all technical actions necessary to reinstate the Participating Agency's ability to participate in the Data Exchange Service including, but not limited to, the reinstatement of the Participating Agency's Digital Credentials. The Coordinating Committee shall inform all the Participating Agencies of such reinstatement.

4. Retention and Dissemination of the E-MOU

The official, executed version of the E-MOU shall be maintained in an electronic form by the Coordinating Committee. The Coordinating Committee shall maintain the E-MOU in a format that is accessible to all E-MOU Participating Agencies.

Appendix 5
Process to Amend the E-MOU

1. Submission of Proposed Amendments to the E-MOU

Any Participating Agency may submit in writing to the Coordinating 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. Approval or Rejection of Proposed Amendments to the E-MOU

If, after considering the request, the Coordinating Committee determines that the request has merit, the Coordinating Committee shall promptly forward the request to the Participating Agencies.

The Coordinating Committee shall meet to vote on proposed amendments to the E-MOU at the next scheduled quarterly meeting, or earlier if deemed necessary by the Chairperson or the Executive Committee.

Once an amendment is approved by the Coordinating Committee, all Participating Agencies shall sign the amendment to the E-MOU prior to the effective date of the amendment.

Appendix 6
Change Process for Data Exchange Services

1. Requests for Change

A. Development Changes

The Coordinating 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 8 of this E-MOU. The Coordinating Committee may appoint a task group to evaluate the Change and provide comments to the Coordinating Committee. The task group may request additional information from the Coordinating Committee or Participating Agencies, as the task group deems reasonably necessary.

B. Compliance Changes

The Coordinating Committee shall have the authority to adopt 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"). The Coordinating Committee may appoint a task group to evaluate the Change and provide comments to the Coordinating Committee. The task group may request additional information from the Coordinating Committee or Participating Agencies, as the task group deems reasonably necessary.

2. Receipt

All requests for Changes shall be directed in writing to the Coordinating Committee Chairperson. The Coordinating Committee Chairperson shall catalog all requests for Changes upon receipt and forward such requests to the Coordinating Committee for consideration.

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 Participating Agencies and their Users; and
g. Copy of the Specification

Appendix 6, Continued
Change Process for Data Exchange Services

3. Evaluation

The Coordinating Committee shall meet to vote on proposed amendments to the E-MOU at the next scheduled quarterly meeting, or earlier if deemed necessary by the Chairperson or the Executive Committee. If the Coordinating Committee appointed a task group for evaluation of the request, the task group shall recommend to the Coordinating Committee whether and how to implement the proposed amendments. The Coordinating Committee shall review the task group's recommendation and take a final vote as to whether the Development Change should be approved.

A. Evaluation Criteria for Proposed Changes

1. Evaluation of Development Changes.

For Development Changes, each Participating Agency shall respond in writing to the Coordinating 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 Participating Agency;
b. whether implementation of the Development Change will require the Participating Agency to materially modify its existing agreements with its Users or third parties;
c. whether the Participating Agency 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 Participating Agency would implement a change (if optional); and
e. whether the implementation would potentially violate applicable law and a description of the potential violation.

The Participating Agency agrees to provide rationale for each response where the Participating Agency responds in the affirmative. The task group or the Coordinating Committee may request additional information from Participating Agencies to further evaluate the responses. If a task group was appointed for a Compliance Change, the task group shall present its findings and recommendations on the Compliance Change to the Coordinating Committee within three (3) weeks of the task group receiving the Compliance Change.

2. Determination of Development Changes.

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 Participating Agencies;
b. whether the change requires at least 20% of Participating Agencies 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 or Committee shall consider the implications of the change to the policies and procedures for the Data Exchange Service.

3. Evaluation of Compliance Changes.

If a task group was appointed for a Compliance Change, the task group shall present its findings and recommendations on the Compliance Change to the Coordinating Committee within three (3) weeks of the task group receiving the Compliance Change.

Any task group shall make recommendations to the Coordinating 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 Participating Agencies should be given to migrate to the new Specification. The Coordinating Committee shall provide an opportunity for affected Participating Agencies 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 Participating Agencies;
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 Participating Agencies related to migrating to the new Specification;
e. The number of Participating Agencies and number of transactions that will be impacted by the new Specification;
f. The amount of time that Participating Agencies 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; and
i. Sunset dates as "old" specifications are retired.

The Coordinating Committee shall review the task group's recommendation and make a final determination regarding the timeline.

B. Response

1. **Development Changes.**

Appendix 6, Continued
Change Process for Data Exchange Services

After the Coordinating Committee approves a Development Change, the Committee shall evaluate whether revisions to the E-MOU will be required and a proposed timeline for implementation. The recommendation of the Coordinating Committee regarding the any revisions to the E-MOU and the proposed timeline for implementation shall be communicated to the Participating Agencies. Revisions to the E-MOU necessitated by approved Development Changes will be performed in accordance with Appendix 5.

2. **Compliance Changes.**

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

Appendix 7
Procedures for Breach Notification

1. Procedures for Notification of a Breach

A. Notification Process

1. Upon initial indication of a Breach that threatens the security of a database and Data communications resulting in exposure of Data, or other incidents compromising the security of the information technology systems with the potential to cause disruption to activities authorized by this E-MOU, the Participating Agency(s) responsible for or affected by the Breach must comply with County procedures to report Breaches to the DIT Information Security Office and HIPAA Breaches to the County HIPAA Compliance Officer, including, but not limited to, by completing the County's Information Security Incident Reporting Form.
2. The Participating Agency(s) responsible for or affected by the Breach will also report the Breach to the Coordinating Committee by emailing the Coordinating Committee Chairperson. Such reports must be made immediately from when the Participating Agency discovered or reasonably should have discovered the occurrence.
3. Upon receipt of the Breach notification, the Chairperson will immediately provide Notice to the members of the Coordinating Committee and affected Participating Agencies, as applicable.
4. Notification of a Breach to the Coordinating Committee does not relieve the Participating Agency of these responsibilities or other responsibilities under Applicable Law, including any required notifications.

B. Notification Content

The Notification to the Coordinating Committee shall include sufficient information for the Coordinating Committee to understand the nature of the Breach. For instance, such Notification shall include the following information, but not limited to:

- one or two sentence description of the Breach;
- description of the roles of the people involved in the Breach (*e.g.*, employees, Users, service providers, unauthorized persons, etc.);
- the specific Data or Type of Data that is the object of the Breach, including whether the Data may have included any confidential or protected Data;
- Participating Agencies likely impacted by the Breach;
- number of Users or records impacted/estimated to be impacted by the Breach;
- actions taken by the Participating Agency 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 7, Continued
Procedures for Breach Notification

The Notification shall not include any confidential or protected Data. The Participating Agency agrees to supplement the information contained in the Notification as it becomes available.

If, on the basis of the information available to the Participating Agency, the Participating Agency believes that it should temporarily cease Data Transmittals with all other Participating Agencies, it may undergo a service level interruption or voluntary suspension in accordance with Appendix 4.

2. Disposition of Breach Alerts and Notifications

A. Review of the Breach by the Coordinating Committee

The Coordinating Committee Chairperson shall facilitate a meeting of the Coordinating Committee upon receipt of the Breach alert or Notification for the purpose of reviewing the Notification and determining the following, in consultation with DIT:

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

B. Determination of Breach Resolution

Once complete information about the Breach becomes available, the Coordinating Committee shall meet to determine whether the Coordinating Committee is satisfied that the Participating Agency(s) have taken all appropriate mitigation measures to resolve the Breach. Upon renewal of any Data Requests, Participating Agencies 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.

1. This resolution will be communicated to all Participating Agency(s) involved in the Breach and those Participating Agencies that ceased Data Transmittals with the Participating Agency(s) involved in the Breach.
2. If those Participating Agencies do not resume Data Transmittals with the Participating Agency(s) involved in the Breach, the Participating Agency(s) involved in the Breach and cessation shall engage in the Dispute Resolution Process.

Appendix 8
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 will be defined and governed by the County's Data Analytics Governance Council and Advisory Group.

Process for Requesting New/Revised Data Services

i. Applicant must submit a request to the Coordinating Committee, in coordination with the Data Analytics Advisory Group. Applicants shall use the template, provided by the Data Analytics Advisory Group, upon an initial request or revision of data from Participating Agencies in accordance with the E-MOU.

ii. The Data Analytics Advisory Group 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 Coordinating Committee will contact the Applicant and request they complete and submit the E-MOU Internal Control Questionnaire ("ICQ"). (ICQ is only required if Participating Agency is receiving Data; not required if solely sending data.)

    1. The Data Analytics Advisory Group shall conduct an initial review of new or revised ICQ within 30 days of its submission and shall make a determination within 30 days, and no longer than 90 days from date of submission as described below in this paragraph. Upon initial review of the ICQ, the Coordinating Committee may request clarification or additional information from the Applicant within 30 days of the submission. Clarification and/or additional information shall be provided back to the Coordinating Committee within 30 days of the request. Review of an ICQ shall take no longer than 90 days in total, however, the Applicant may request an extension of the review period from the Coordinating Committee in writing before the 90 day review period expires.
    2. If the ICQ is approved, the Applicant shall begin to draft a Specification and requirements based on the Coordination Committee and the Data Analytics Advisory Group.

Attachment A to Appendix 8

USER ACKNOWLEDGEMENT FORM

INDIVIDUAL'S 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 E-MOU is confidential and must be protected from unauthorized disclosure and use. I have been provided access to a copy of the E-MOU and agree to abide by the same restrictions and conditions that apply to User with respect to the Data. I have been instructed by the Participating Agency on the permissible use(s) of the Data and will not use the Data for any other purpose. Participating Agency has provided me with a list of the individuals or Agencies 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 Participating Agency who are not authorized to access the Data. I have received instructions from Participating Agency 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 Coordination Committee. 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:

Name and Title:_____

Date_____