Data Use Agreement (DUA) Attachment Outlines & Instructions

Typically, the Data Use Agreement includes the following seven (7) attachments comprised of information submitted to Medicaid Planning by the data requestor: (1) Attachment A1: Covered Data & Period of Use; (2) Attachment A2: Scope of Work; (3) Attachment A3: Additional Data Sources; (4) Attachment A4: Data Users; (5) Attachment A5: Data Management Plan; (6) Attachment A6: Data Storage Location; and (7) Certificate of Data Destruction.

Attachment A1: Covered Data & Period of Use

[This is part of DUA]

This text of this attachment must include the abridged name of data provider's legal entity and abridged name of data requestor's legal entity. It must identify via a bulleted listing all covered data sets. It must define the targeted time periods of the stored data to be released and the periodicity (i.e., recurring frequency) of the data releases. If a defined data dictionary is known, a reference to this attached data dictionary is to be included. This data dictionary, if any, is to be attached to the DUA. If there is to be a separate agreement between the legal entity of the data requestor and the legal entity of the data provider for financial compensation of the data provider, the parties and their duties and responsibilities must also be delineated.

[*Send Draft Attachment A1 to: mdh.medicaiddatarequests@maryland.gov*]

Attachment A2: Scope of Work

[This is part of DUA]

This text needs to address how the abridged name of data requestor's legal entity will use the Medicaid data. It must clarify which entities will receive periodic reports of analyzed and interpreted data, and what types of measurement, analysis and assessment support will be provided by which parties. It must include a bulleted outline of the specific metrics that will be examined and presented in the reports. The text is to include a statement that when necessary the abridged name of the data requestor's legal entity will specify additional metrics to be obtained, and how these additional metrics will be incorporated into the suite of previously identified measures and reports.

[*Send Draft Attachment A2 to: mdh.medicaiddatarequests@maryland.gov*]

Attachment A3: Additional Data Sources

[This is part of DUA]

This text presents a bulleted listing of additional data sets to be provided by sources other than Maryland Medicaid and its contracted data provider. A brief description of each additional data set and its organizational source is to be included for each item listed.

[*Send Draft Attachment A3 to: mdh.medicaiddatarequests@maryland.gov*]

Attachment A4: Data Users

[This is part of DUA]

A table comprised of the following column headers is to be constructed: (C1) Last name of data user, (C2) first name of data user, (C3) organizational affiliation of data user, (C4) office telephone of data user and (C5) email address of data user. Each anticipated data user is to be identified in a separate row of this table. In the text accompanying this table, it is stated that the abridged name of the legal entity of the data requestor--and its sub-contractor (if any) also identified by its abridged legal entity name--agrees to access the requested data only as needed and that all data users are subject to all security protocols, policies and requirements necessary to safeguard shared data. The abridged name of the legal entity of the data requestor also indicates that the included roster of individual data users will be updated, as needed.

[*Send Draft Attachment A4 to: mdh.medicaiddatarequests@maryland.gov*]

Attachment A5: Data Management Plan

[This is part of DUA]

Introduction paragraph: This paragraph must name the parties involved in the DUA and outline what type of data the requesting party is receiving. Also, list the entities and/or the individual users of organizations to which/whom data access is limited. The purpose of the Data Management Plan is to ensure confidentiality and protection of protected health information (PHI) contained in the data sets. The details of the data management plan are outlined below.

1. **Data Requested**

A summary needs to be provided, or if a part of another attachment in the DUA, reference to that Attachment.

2. **Data Receipt and Storage**

This section must describe where and how the data is to be hosted, received, analyzed and stored. If the requesting party is using another company to host, receive, store and analyze the data, that company must be mentioned by name. Access to data requires two factor authentication and role-based credentialing. The data storage company must be named and must ensure that all data sets are housed in advanced, robust technical environments that are fully compliant with standards described in the Federal Information Security Management Act of 2002 (FISMA) and National Institute for Standards of Technology (NIST) section 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations.”

This section must describe the steps the requesting party will take to securely transfer the hosted data from the targeted data provider to the requesting party’s data storage location. It must mention that if any data was temporarily stored by an intermediate party en-route to the final, secured destination, the

temporarily stored data must be destroyed immediately upon completion of the data transfer to the requesting party's data storage location. Pursuant to the requirements in the DUA, the requesting party must provide a completed and fully executed Certificate of Data Destruction (included as an attachment to this DUA) to Medicaid within 30 days of the data destruction date. The destruction process shall meet data destruction standards as specified by the National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitation (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf).

The requesting party also agrees that upon termination of the agreement, the requesting party shall destroy all data stored at the data storage location immediately, in the manner set forth in the aforementioned paragraph and DUA.

3. Data Access, Use and Protection

This section will focus on the requesting party's usage of the Medicaid data files within a closed environment. It will specify how the received data sets will be stored on secure, limited-access networks that are password protected to ensure that access to the data is limited to individuals working on specific tasks that actually need the data accessed.

4. Data Users

This section will highlight the requesting party that is responsible for organizing and storing the Medicaid data. This section must list the names and titles of the project director, who has ultimate responsibility for hosting and maintaining the data, and the project manager. These two individuals will assign qualified staff to analyze the Medicaid data, and share data with its subcontractor, as needed, to support project deliverables.

This section will address who will be the designated custodian of the data provided. The specific years of custodianship should be listed. The data will only be available to the requesting party and its subcontractor. Only the named users of the requesting party and its subcontractor (who all must be listed in the DUA as a separate attachment) will be granted access to the data stored in the aforementioned data storage location.

This section will discuss how individual users must be included in a separate agreement and approved by the Project Director before accessing sensitive data. Upon execution of the DUA, the requesting party will create a list of users with access to the Medicaid data and all data users will complete the Data Use Agreement Addendum. The requesting party will implement the following protocol to track users and access:

- Maintain an inventory of individuals authorized to have access to the Medicaid data housed in the listed data storage company environment in an Excel spreadsheet. The spreadsheet will include a list of all project team members' contact information and start date.

- Only project staff assigned to analyze Medicaid data will have access to directories where Medicaid data sets are stored. The default data storage company's security features provide each user the same permissions to the projects shared folder. The requesting party will request that the administrators of the data storage company create secure directories specifically for the users of the users of the requesting party and its subcontractor who will have access to the Medicaid data based on their assigned roles.

- Rescind individual's access to the Medicaid data folders upon the team member's termination of the engagement.

[*Send Draft Attachment A5 to: mdh.medicaiddatarequests@maryland.gov*]

Attachment A6: Data Storage Location

[This is part of DUA]

The manager and site of stored data is defined by abridged legal name and location. A statement of assurance that the data storage company will share data only with authorized data users must be included, along with an assurance that the data storage company will ensure that all shared Medicaid data are to be housed in advanced, robust technical environments that are fully compliant with standards described in the Federal Information Security Management Act of 2002 (FISMA) and National Institute for Standards of Technology (NIST) section 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations." If applicable, a statement that each shared data set will be temporarily stored by the abridged legal entity name of the data requestor in a secure network drive that will only be used for the purpose of receiving data from Medicaid's contracted data provider (which is also named) is to be included. A statement that once data have been fully received, the abridged legal name of the data requestor shall transfer the datasets to the abridged legal name of the data storage company and shall destroy all data previously saved in the abridged legal name of the data requestor's secure network drive in a timely manner is also to be included. A statement that the abridged legal name of the data requestor shall send a fully executed Certificate of Data Destruction (to be attached to the DUA separately) to Maryland Medicaid and the abridged legal entity name(s) of other relevant party or parties following data transmission within 30 days of the data destruction date is also to be include.

[*Send Draft Attachment A6 to: mdh.medicaiddatarequests@maryland.gov*]

Attachment A7: Certificate of Data Destruction

MDH Planning will append a blank certificate to the DUA.