Policy and Procedure Manual

POLICY NAME: Internal Data Sharing
POLICY NUMBER: A09-04
ISSUE DATE: July 2015
REVISED DATE: September 2018

PURPOSE:

1. To ensure that data team recipients are authorized to receive the data requested from internal UCM/BSD sources.

2. To establish the Office of the Chief Analytics Officer as the centralized function to direct data team requests to the analytics group best positioned to fulfill a request.

3. To require that where a business oriented analytics team exists, that analytics team should provide data to those business customers that meet the terms of use of the request and assist in determining if the Data Team Recipient is authorized to access the requested data.

4. To ensure transparency of data exchanges through reliable tracking methods and documentation.

DEFINITIONS: (if applicable)

1. **DataTeam Provider** means an authorized representative of a business oriented analytics team of UCM/BSD that owns and/or transforms data for business customers.

2. **Data Team Recipient** means a representative of a business oriented analytics team of UCM/BSD authorized to have access to the data and is not the business user of the data requested.

3. **Data Sharing** means the data team provider provides data in one of three ways: 1. The data team provider has transformed available data, using processes, software, and / or expertise in a way that adds value, 2. The data team provider is the owner of data that is otherwise non-existent at UCM/BSD, 3. The data team provider is the owner of data AND transforms the data using processes, software, and / or expertise in a way that adds value that is otherwise non-existent at UCM/BSD

POLICY:

1. For internal data sourcing, there will be a Data Team Provider and Data Team Recipient.

2. Data Team Providers, and authorized representatives within their UCM/BSD reporting structures, (provider) are permitted to share data with Data Team Recipients, and authorized representatives within their UCM/BSD reporting structures, (recipient):

    a. Where the inability of access stems not from permissions to access but because of the existing skillset or software tools to access the data, the Data Team Recipient displays existing access approval through the demonstration of access to the building blocks of the data to be shared (e.g., UB04 billing data are the building blocks for AHRQ Indicators.)

    b. Where the user's inability to access data stems from either a financial or legal barrier (typically involving a business associates agreement (BAA) or data use agreement (DUA)), demonstration must be presented to and data access granted by the Data

Governance Council. The Data Governance Council may create alternate policy or procedures for other specific circumstances.

3. The use of the data shared is limited to the terms agreed upon by the Data Team Recipient and Data Team Provider for the original request. A new request for data specifying different terms of use must be filed in the event that the Data Team Recipient finds a need to: 1. add previously unspecified end-users to the data products that they have created with the data shared by the Data Team Provider, or, 2. create previously unspecified data products with the data shared by the Data Team Provider.

4. This policy does not address compensation for access to data sources from the recipient party to the provider party. The recipient and provider parties involved will negotiate compensation in the form of in-kind services (i.e., quid-pro-duo access to a data source) or through other means.

PROCEDURES:

1. The Data Team Recipient enters a data request in the ACReS system.

2. Once the request is received, it will be routed to the most appropriate analytics team at UCM or BSD to be the designated DataTeam Provider.

3. The Data Team Provider and Data Team Recipient will review the reasons for inability to access the data where Data Provider will provide clear indication of which data elements are available and to what extent the sources are available.

   a. Where data access permissions are demonstrated, the Data Team Provider will fulfill the data request in the usual manner for that team.

   b. Where financial or legal barriers exist, the data request will be forwarded to the Data Governance Council for review and decision.

      i. The Data Governance Council will collect background information from Data Team Recipient and Data Team Provider(s).

      ii. The Data Governance Council may create alternate policy or procedures to support these specific circumstances.

      iii. The Data Governance Council will communicate the decision to the Data Team Recipient and Data Team Provider(s).

4. If the Data Team Provider cannot meet the need, then the Data Team Provider will discuss this with the Data Team Recipient and determine next steps. Next steps may include denying the request, redirecting the request to another qualified data team, or escalating the request for review by the Analytics Core.

   a. The Analytics Core is defined as leaders from:

      i. Department of Data & Analytics

      ii. Office of Managed Care

      iii. Chicago Biomedicine Information Services

      iv. Center for Research Informatics

      v. University of Chicago Physicians Group

5. Data Team Recipient notifies the Office of the Chief Analytics Officer to update the ACReS

request to reflect the following:

      i.   Who the Data Team Provider and Data Team Recipient are

     ii.   The type of data shared

   iii.   The medium by which data are delivered

   iv.   The terms of use, including the data products to be created and the end-users to be given access by the Data Recipient with the data shared

6. Once routed to a specific team, the request will then be handled as it typically would for that team and is subject to the policies and procedures of that particular team. These include and may not be limited to request for additional information, IRB approval and chargeback. This process will also require that all data team providers and data team recipients confirm awareness and adherence to data security, HIPAA and device encryption policies at UCM.

7. Where applicable, the Data Team Provider will help facilitate regulatory obstacles associated with accessing data sources. This includes assistance with data use agreements, submission and facilitation of hardware and software firewall change requests to appropriate security teams, as well as other barriers to access.
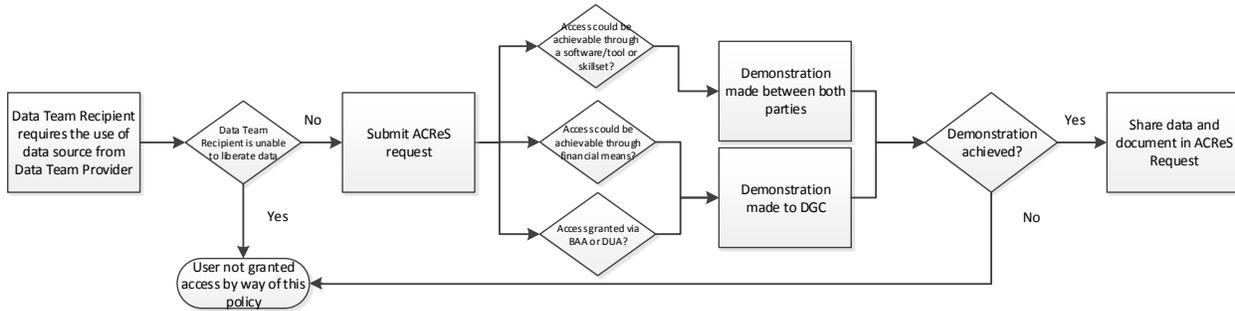

Figure 1: Data Sharing Request Procedure

INTERPRETATION, IMPLEMENTATION, AND REVISION:

The Data Governance Council is responsible for the interpretation and revision of this policy. Data Governance Council leadership are responsible for the implementation of this policy.

REFERENCES: (to outside sources, if applicable)

CROSS-REFERENCES: (to other UCH policies, if applicable)

1. See policy on acceptable mechanisms for data sharing provided by the Office for Information and Security.

2. Policy number: A05-12, Permitted Uses and Disclosures to Carry Out Treatment, Payment and Health care Operations

_____

Sharon O'Keefe
President