POLICY
Approved - 9.9.14

Extraction of Identifiable Data from the Information Exchange

Purpose

To create a governance process to manage requests to extract identifiable data from the Information Exchange (IE).

Background

Several use cases have been identified that require the extraction of identifiable data from the IE. Those cases are categorized as follows:

1) Extraction required to use computational power or applications not available within the IE, or
2) Extraction required to share with other data (such as with data at another research institution, data already existing in another physical location that cannot reasonably be moved, reporting to a data registry).

To create efficiencies and better serve our constituents, we request approval of this process so that those requesters meeting the requirements of the process would not need to receive individual approval from the Executive Leadership & Governance Committee for extraction of data. The process would be limited to allow extraction of identifiable data only for the use cases described above, and in accordance with the requirements described below.

Evaluation and Oversight

Requests for data extractions will be tracked as part of the overall data request process. Information tracked includes all data fields entered for the request, as well as total number of requests, categories of request (computation, data sharing), and number of requests fulfilled.

Reporting on data extraction will be available to the data stewards of participating organizations (currently Fairview, UMP and UMN) on demand through AHC-IS.
Data Request Form Modifications

The current request form to request data will be modified to support this process. Expected changes to the request form will likely include adding fields to support additional information on the need for the extraction of the data and how the data will be handled following extraction.

General Requirements for Extraction (applicable to all Scenarios):

Requester must:

• Have an x500 userid; and
• Have completed HIPAA training.

Extraction must be for purposes of:

• IRB approved research;
• Fundraising as permitted under HIPAA;
• Healthcare operations (other than fundraising) as permitted under HIPAA; or
• Reporting as required under state or federal law;

AND

• Extraction of data is necessary due to a need to:
  o use computational power or applications not available in the IE shelter; OR
  o share with other data not in the IE (such as with data at another research institution, data already existing in another physical location that cannot reasonably be moved, reporting to a data registry).

Specific Requirements:

Scenario 1 – IRB Approved Research

The following criteria must be met:

• There must be patient authorization to use the data, or a waiver for patient authorization from the IRB.
• The data must be accessed only by those who are adequately described in the patient authorization or applicable IRB documentation.

• The data must be used only for the purposes described in the patient authorization or applicable IRB documentation.

• Any data that is extracted to reside at UMN/UMP/FV must meet the following criteria:
  
  o any data residing at UMN must reside on an AHC-IS supported computer or server, or another computer or server that meets HIPAA Security standards as determined jointly by UMN’s Chief Health Information Compliance Officer and Chief Information Security Officer;
  
  o any data residing at UMP must reside on a UMP-IS supported computer or server; and
  
  o any data residing at FV must reside on a FV-IS supported computer or server.

• Any data that is extracted to reside at any location other than UMN/UMP/FV must be subject to a business associate agreement, data use agreement or such other form of agreement approved by the appropriate authority at UMN/UMP/FV. Where either a data use agreement or other form of agreement is approved and entered into, such agreement will specifically provide that the recipient of the data will:
  
  o Have a security program in place that is subject to an assessment process or a third party audit;
  
  o De-identify data for processing where appropriate;
  
  o Control access to the data appropriately;
  
  o Use data transport and storage encryption as appropriate;
  
  o Segregate the data from other data where feasible;
  
  o Ensure that the data does not reside on a system that has internet connection, or, if internet connection is necessary for the purposes of the engagement, then ensure that appropriate system protection, patch mechanisms and controls are in place and monitored;
  
  o Ensure that any data removed from the system has the same level of protection as data residing on the system; and
  
  o Destroy the data when no longer needed (and destruction is feasible) and provide a certification of destruction upon request.
Scenario 2 – Fundraising

The following criteria must be met:

- Only the information permitted to be used for fundraising under HIPAA regulations may be extracted (Note: AHC-IE maintains the table of permitted fields as approved by UMN/UMP/FV).

- Patients who request to be opted out of fundraising must be excluded (Note: AHC-IE performs this cross-check as to EPIC in advance of releasing the data; UMF performs additional cross-checks against its own opt-out lists).

- Data residing at UMF must reside on a UMF-IS supported computer or server. UMF will utilize UMN OIT services for security as appropriate, and will provide UMN with security assessment and audit results as requested.

- Data that is extracted to reside at any location other than UMF must be subject to a business associate agreement, or a confidentiality agreement that requires the recipient to:
  - Have a security program in place that is subject to an assessment process or a third party audit;
  - De-identify data for processing where appropriate;
  - Control access to the data appropriately;
  - Use data transport and storage encryption as appropriate;
  - Segregate the data from other data where feasible;
  - Ensure that the data does not reside on a system that has internet connection, or, if internet connection is necessary for the purposes of the engagement, then ensure that appropriate system protection, patch mechanisms and controls are in place and monitored;
  - Ensure that any data removed from the system has the same level of protection as data residing on the system; and
  - Destroy the data when no longer needed (and destruction is feasible) and provide a certification of destruction upon request.
Scenario 3 – Healthcare Operations

The following criteria must be met:

• The data must be for healthcare operations as defined under HIPAA, including:
  o quality assessment and improvement activities, patient safety activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination;
  o reviewing qualifications and evaluating practitioner/provider performance, training, accreditation, licensing, certification or credentialing.

• The data must be accessed only by those actively involved in the operations described in the original request, and only for the purpose of the operations described in the original request.

• Any data that is extracted to reside at UMN/UMP/FV must meet the following criteria:
  o any data residing at UMN must reside on an AHC-IS supported computer or server, or another computer or server that meets HIPAA Security standards as determined jointly by UMN’s Chief Health Information Compliance Officer and Chief Information Security Officer;
  o any data residing at UMP must reside on a UMP-IS supported computer or server
  o any data residing at FV must reside on a FV-IS supported computer or server

• Any data that is extracted to reside at any location other than UMN/UMP/FV must be subject to a data use agreement or business associate agreement, or such other form of agreement approved by the appropriate authority at UMN/UMP/FV. Where either a data use agreement or other form of agreement is approved and entered into, such agreement will specifically provide that the recipient of the data will:
  o Have a security program in place that is subject to an assessment process or a third party audit;
  o De-identify data for processing where appropriate;
  o Control access to the data appropriately;
  o Use data transport and storage encryption as appropriate;
  o Segregate the data from other data where feasible;
  o Ensure that the data does not reside on a system that has internet connection, or, if internet connection is necessary for the purposes of the engagement, then ensure that appropriate system protection, patch mechanisms and controls are in place and monitored;
  o Ensure that any data removed from the system has the same level of protection as data residing on the system; and
  o Destroy the data when no longer needed (and destruction is feasible) and provide a certification of destruction upon request.
Scenario 4 – Reporting as Required Under Law

The following criteria must be met:

• The requester for the extraction must provide the citation or general reference to the law that requires reporting.

• Appropriate authorities (legal and/or compliance) at UMN/UMP/FV will review the legal requirement and if reporting is required, the requirement will be documented (including fields of information to be reported and frequency of reporting) and provided to ICS and IE for future reference.

• Once a requirement is documented, the extraction may proceed on a recurring basis as is required under law.