

Extraction of Identifiable Data from the AHC Information Exchange

Responsible University Officer: Clinical and Translational Science Institute Biomedical Informatics Director

Policy Owner: Constantin Aliferis, califeri@umn.edu

POLICY STATEMENT

To create efficiencies and better serve our constituents, this policy permits the extraction of identifiable data from the AHC Information Exchange (IE) for those use cases that meet the criteria described herein, without approval from the Executive Leadership & Governance Committee (the "Committee") for each individual request. Use cases that do not meet the criteria described in this policy must be approved by the Committee before extraction can be performed.

Use cases that would require the extraction of identifiable data from the IE are as follows:

1. Extraction required to use computational power or applications not available within the IE secure data environment, or
2. Extraction required to compile 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)

General Requirements for Extraction

1. 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
2. Extraction of data is necessary due to a need to:
 - use computational power or applications not available in the IE data shelter; or
 - compile 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);
- AND
3. Requester must be an Authorized User per the AHC-IE Data Access and Use Policy (at a minimum, requester must have an x500 User ID and must have completed HIPAA Training)

Clinical and Translational Science Institute

Specific Requirements

IRB Approved Research

The following criteria must be met:

- There must be patient authorization to use the data, or a waiver of patient authorization from the IRB. For research relying on a waiver of patient authorization, information on patients who have elected to opt out of research will not be included in the data to be extracted.
- The data must be accessed only by those who are adequately described in the patient authorization or applicable IRB submission.
- 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 the University of Minnesota (UMN), University of Minnesota Physicians (UMP) or Fairview (FV) must meet the following criteria:
 - Any data residing at UMN must be stored on a Health Sciences Technology (HST) 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;
 - Any data residing at UMP must be stored on a UMP-IS supported computer or server;
 - Any data residing at FV must be stored on a FV-IS supported computer or server.
- Any data that is extracted to reside at any location other than UMN/UMP/FV must meet the following criteria:
 - The recipient of the data must be a federal agency (such as NIH), an organization coordinating a federally registered clinical trial, or a U.S. research organization that receives at least \$100 million in funding from NIH annually; and
 - The extracted data must meet the definition of a "limited data set" under HIPAA, and the recipient of the data must enter into a form of Data Use Agreement that meets HIPAA requirements. All review and approval processes for Data Use Agreements of the organization requesting the data extraction (UMN/UMP/FV) must also be followed.

Fundraising

Extraction of data for purposes of fundraising may be done at the request of the University of Minnesota Foundation (UMF), provided that the following criteria are be met:

- Only the information permitted to be used for fundraising under HIPAA regulations may be extracted (Note: BPIC maintains the table of permitted fields approved by UMN/UMP/FV).
- Patients who request to be opted out of fundraising must be excluded (Note: BPIC performs this cross-check from EPIC in advance of releasing the data; University of Minnesota Foundation (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;

Clinical and Translational Science Institute

- 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

Healthcare Operations

The following criteria must be met:

- The data must be for healthcare operations as defined under HIPAA, including:
 - 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;
 - Reviewing qualifications and evaluating practitioner/provider performance, training, accreditation, licensing, certification or credentialing.
- The data steward for the organization requesting the data extraction (UMN/UMN/FV) must be consulted to ensure that the data being requested meets both HIPAA and any organizational requirements for healthcare operations data.
- 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 must reside at the University of Minnesota (UMN), University of Minnesota Physicians (UMP) or Fairview (FV), and must meet the following criteria:
 - Any data residing at UMN must be stored on a Health Sciences Technology (HST) 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;
 - Any data residing at UMP must be stored on an UMP-IS supported computer or server;
 - Any data residing at FV must be stored on a FV-IS supported computer or server.

Reporting as Required Under Law

The following criteria must be met:

- The requester 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 IE personnel for future reference.
- Once a requirement is documented, the extraction may proceed on a recurring basis as is required under law.

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 presented to the Committee by staff from the Best Practices Integrated Informatics Core (BPIC) of the University's Clinical and Translational Science Institution on a quarterly basis, in the form and format requested by the Committee, and will also be available at other times upon request by the data stewards of participating organizations (currently Fairview, UMP and UMN).

This *Extraction of Identifiable Data from the Information Exchange* policy will be presented to the Committee by BPIC on a regular basis for review.

REASON FOR POLICY

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

PROCEDURES

Requests to extract data from the IE secure data environment will be submitted to the Data Shelter File Transfer application.

1. Login to the AHC-IE Data Shelter
2. From any browser, go to the URL: <https://portunus.ahc.umn.edu>
3. Sign in using your x500 username and password
4. Approve dual authentication
5. Select your project
6. Specify the reason for extracting the file
7. Upload file to be extracted*

*Note: Files leaving the data shelter will need to be approved before they are available to download

FORMS/INSTRUCTIONS

Instructions can be accessed here - <https://confluence.ahc.umn.edu/display/POR/File+Transfers>

APPENDICES

There are no appendices associated with this policy.

FREQUENTLY ASKED QUESTIONS

There is no FAQ associated with this policy.

Clinical and Translational Science Institute

ADDITIONAL CONTACTS

Subject	Contact	Phone	Email
Primary Contact	Gretchen Sieger	612.626.7495	siege022@umn.edu
Alternate Contact	Steve Johnson	612.625.7940	joh06288@umn.edu

RELATED POLICIES AND PROCEDURES

University of Minnesota Administrative and Board of Regents Policies:

- [Protected Health Information](#)
- [Protection of Individual Health Information](#)
- [Research Data Management: Archiving, Ownership, Retention, Security, Storage, and Transfer](#)

University of Minnesota Administrative Procedures:

- [Destruction of University Records](#)

Clinical and Translational Science Institute Policies and Procedures:

- AHC-IE Data Access and Use Policy
- [BPIC Data Request Procedures](#)

REFERENCE

NIH Awards by Location and Organization

- <https://report.nih.gov/award/index.cfm>

POLICY HISTORY

Policy Created: 9/9/2014

Policy Revised: 6/16/2020