ENACT STANDARD OPERATING PROCEDURES V7.5

SOP 1: Adding New or Modifying Existing Data Domains

Introduction: The Data Harmonization Workgroup has defined a set of data domains (e.g., Demographics, Diagnoses, Procedures) and standards for representing data in those domains. As the project evolves, there may be the need to both modify existing domains and/or add new data domains (e.g., new laboratory test orders, results). The process steps listed below are designed to facilitate the objective of the SOP while allowing for thorough and thoughtful consideration by all parties involved in ENACT.

1. Request for a modification or addition of a data domain is submitted to the ENACT Data Harmonization Work Group (DHWG) by a participating ENACT Network Site or an ENACT Work Group.
2. The request is circulated to all members of the DHWG for review.
3. The DHWG discusses the request and revises or modifies it as the membership sees fit.
4. The request is submitted to the Technology Work Group (TWG) and Network Operations team for their review and recommendation as to the feasibility of implementing the request.
5. Assuming a favorable recommendation from the TWG and Network Operations team, the members of the DHWG vote to approve or deny the request. Approval by a simple majority of ENACT Network Sites as represented by DHWG group members is required.
6. Approved requests are forwarded to the ENACT Executive Committee for approval before they can move forward with implementation.
7. Decisions not to approve an application will be accompanied by a detailed explanation from the ENACT Executive Committee.
8. If the DHWG denies the request, the applicant site may appeal to the ENACT Executive Committee. If the ENACT Executive Committee denies the request, the applicant site may appeal to the ENACT PI Group.

SOP 2: Process for User Registration and Management

Introduction: The principle upon which this SOP is based is that no user may use the ENACT Network without authorization by a participating ENACT organization that takes responsibility for the user's actions. The mechanisms for authorization are based on the Harvard SHRINE model. This model assumes that the ENACT Network is a version of a federated network where any given participating organization may authorize individuals to use the network based upon the conditions specified in the "ACT Network Site Agreement." Furthermore, it is assumed that every other participating organization agrees to honor this authorization and agrees to provide access to that organization's information as defined in the ACT Network Site Agreement. SHRINE provides the technical means to implement this SOP through secure trust relationships (certificates) from each site and association of local user ID (from the originating site) with all queries that allow traceability of individual user's activity to all sites. The details below describe the process of local user registration at each site that must be undertaken to implement the Terms of Data Access.

1. Each site must formulate a set of criteria and create processes for Qualified Faculty, supervised Fellow or Qualified Staff for registering and monitoring that conform to the Terms of Query Access.
2. A description of these criteria and process descriptions must be made available to the Network Operations team before a site onboards to the ENACT production network.

3. Each site is responsible for managing User Registrations and for de-authorization when a user no longer meets the criteria for use (for example, their employment is terminated by the authorizing member) or is deemed by the Data Steward (either at the ENACT site or ENACT's Data Steward) to have misused the network.
4. Noncompliance: The SHRINE network is designed to restrict inappropriate use of the network (e.g., attempting to re-identify individuals from within the data sets). The SHRINE system implements security mechanisms such as query result obfuscation, active monitoring and access controls to help identify and prevent inappropriate use. Key to the effective use of these security mechanisms is the role of a site Data Steward. An ENACT site's institutional or ENACT Data Steward is responsible for that site's users. SHRINE enables each site's Data Steward to access and control these security mechanisms. Some of these mechanisms function automatically (e.g., identification and locking out users who perform repeated queries that might be used for re-identification) and others require manual intervention by the Data Steward and/or IT system administrators across the network. A Data Steward may be called upon to restrict access or confirm a previously applied automatic access restriction for a user. They may also be called upon to remove automated access restrictions where the behavior of the user is determined to be legitimate. They will communicate with other Data Stewards and/or IT system administrators as needed to implement or remove these access controls.
5. Any review of network use is at the discretion of the ENACT Executive Committee, and any decisions rendered should be considered final and binding.

SOP 3: Monitoring and Auditing

Introduction: In order to determine if the ENACT Network is achieving its goals, that sites are participating in accordance with the network agreement and that users are not engaging in abuse of the network, it is necessary to establish a Monitoring and Auditing function. This requires that information about the functioning of the network be archived in some manner and that reporting mechanisms are created to analyze and summarize this information.

To track functioning of this network, a central archive of high-level network transactions is needed. At the same time, it is also important to protect the confidentiality of researcher queries by limiting the information in this archive to only those characteristics of the transactions or queries that are relevant to monitoring and auditing.

The following defines the process of collecting this information, including the metadata that will assist in the monitoring and reporting process. For purposes of this SOP, the originating site is the ENACT site where the query is initially constructed and that initiates distributing of that query to other network sites. The receiving site is any site that receives the query, executes that query with respect to their local data and returns the results to the originating site.

1. ENACT will establish and maintain a central query metadata archive for the purpose of monitoring, auditing and reporting ENACT network activity. This central archive will continue to be enhanced over time with new releases of the SHRINE software.
2. All queries and their associated metadata may also be archived at both the originating and responding sites.
3. The query metadata to be collected will be:
   a) From the Originating Site
      i) ENACT unique site identifier
      ii) Site unique faculty identifier(s)

        iii) Site unique query identifier
        iv) Date-time stamp of the query transmission
        v) Query intent
    b) From the Receiving Site
        i) Items i – iv above
        ii) Receiving Site unique query identifier
        iii) Query receipt date-time
        iv) Query execution date-time
        v) Receiving site identifier
        vi) Results transmission date-time
        vii) Time to execute query
4. All query archives should be considered protected information and only accessible to authorized individuals for a set of agreed upon purposes.
    a) Monitoring and reporting on system activity
    b) Detecting and reporting abuse of the system
5. The local Data Steward is responsible for monitoring queries in order to determine if they conform to the Terms of Query access. Any queries that do not conform will be reported to the ENACT Executive Committee for review and possible action. The action will be taken at the ENACT Network Site that is the origin of the reported query.
6. A report of ENACT SHRINE query activity and associated system use will be provided to the ENACT Executive Committee and to each participating ENACT Network Site on a to be determined basis, as set forth by the ENACT Executive Committee and Evaluation team.

SOP 4: Research using deidentified aggregate data

Introduction: In accordance with the ENACT Aims, as of February 1st, 2023, an amendment to the original ACT Network Agreement permits research to be conducted across the network's deidentified data. This amendment enables access to all network deidentified data for purposes of cohort exploration, analysis, and publication.

1. Use cases for the network have expanded beyond cohort exploration to include analysis of this cohort and subsequent publication of results. Publication guidance is covered in SOP 5.
2. Research is defined as: Clinical, translational, population health and outcomes research of common and rare and neglected diseases as well as other research focused on human health that is enabled by using aggregated de-identified data.
3. Network users: All elements of SOP 2, above, apply. Each institution is responsible for the conduct of their investigators whom they provided access to ENACT. The Terms of Query Access must be signed off by each new user to the network. Sites are required to have data stewards regularly monitor network activity of their own end users and reporting concerns to the institution or central ENACT project teams.
4. Network monitoring: All elements of SOP 3, above, apply.

SOP 5: Publication

Introduction: To ensure sound use of the ENACT network data and subsequent analyses for publication, initial guidelines have been put in place. These guidelines will be regularly reviewed and refined by the ENACT Governance Work Group to ensure publication best practices are in use.

1. All collaborators and data contributing sites must be acknowledged by using the appropriate CTSA Hub grant number from participating institutions.
2. Any Intellectual Property derived from the use of the ENACT Network must cite the NCATS ENACT grant: “This project was supported by the National Institutes of Health through grant 1U24TR004111-01.”
3. Publications may not disclose any information that could potentially identify a data source partner (ENACT site), including site name, patient population characteristics, or geographic characteristics, unless explicitly approved by the data source partner in writing, prior to submission of a manuscript. Such approval must be requested and received in writing between the requestor and the Senior Vice President of Research, the Chief Information Officer, their respective designee, or similar leadership position at each institution whose data are used in the publication. Any entity (e.g., hospital) that does not agree to be identified by name as a data source will be instead identified as a “CTSA-affiliated site.”
4. ENACT Publication Approval Process: Publication requests will be reviewed and approved by the ENACT Publication Committee before submission. Steps are listed below.
   a) Investigators should complete this form (*to be created*) with information including:
      i) Investigator(s) name and institution(s)
      ii) Area of study
      iii) Proposed publication title
      iv) Data analysis methods
      v) Findings
      vi) Data contributors (entire network? Select institutions?)
      vii) Validation of data quality (what checks have been done to confirm data quality is acceptable for purposes of this analysis?)
      viii) Confirmation that local BERD teams will review the analyses and provide support where necessary, ultimately singing off on the analyses
   b) The ENACT Publication Committee, selected by ENACT PIs and Governance Work Group Members, will review requests and follow up via email with questions, and approval or denial for publication, with explanations as appropriate.
   c) The investigator must reference steps 1 through 3 for appropriate attributions.

SOP 6: Use and Management of Ephemeral Enclaves (or Process for User Registration and Management for Ephemeral Enclaves)

Introduction: This SOP lays out the operating procedures ephemeral data enclaves through the ENACT Network. The ephemeral data enclaves will serve as a data repository for health data for research purposes defined in SOP 4. The governance and structure of these enclaves is further described in the ENACT Limited Data Set Enclaves Data Transfer Agreement and the UCSD ENACT Data Enclave Infrastructure Management Plan.

1. Ephemeral data enclaves may only be requested and used by authorized ENACT Network users (as defined in SOP 2 under the Harvard SHRINE model), employed at institutions that have signed the ENACT Limited Data Set Enclaves Data Transfer Agreement.
2. Ephemeral data enclaves may be requested through a REDCap form accessible through SHRINE.
3. All ephemeral data enclave investigators must have academic appointments or be employed by an ENACT site that has signed the ENACT Limited Data Set Enclaves Data Transfer Agreement.
4. All ephemeral enclave requests must be approved by the ENACT Protocol Review Committee.

5. All administration, management, monitoring, and operation activities for ephemeral data enclaves will be handled centrally by the University of California – San Diego.
6. Any research conducted in the ephemeral data enclaves must follow the research guidelines in SOP 4.
7. Any publications written based on ephemeral data enclaves must follow all guidelines in SOP 5.
8. In addition, all publications must explicitly acknowledge that ENACT enclaves are closed access, with users being barred from removing data from the enclaves under any circumstances.