JOHNS HOPKINS MEDICINE	Johns Hopkins Medicine **JHM Data Trust Guidelines** **General**	*Policy Number*	GEN001
		Effective Date	07/20/2018
	Subject **Guidelines and Technical Requirements for Registries**	*Page*	1 of 3
		Supersedes Date	09/19/2017

This document applies to the following Participating Organizations:

Howard County General Hospital	Johns Hopkins Bayview Medical Center	Johns Hopkins Community Physicians	Johns Hopkins HealthCare LLC
Johns Hopkins Home Care Group	Johns Hopkins Medicine International	Johns Hopkins School of Medicine	Potomac Home Health Care
Sibley Memorial Hospital	Suburban Hospital	The Johns Hopkins Health System Corporation	The Johns Hopkins Hospital

Keywords: clinical registry, data management, data trust, quality registry, registries, research registry

Table of Contents

I. RATIONALE

A **registry** is an organized system that uses observational study methods to collect granular data from a population defined by a **particular disease, diagnosis, condition, exposure or experience**, and that serves one or more **predetermined scientific or clinical purposes**. This document applies to all JHM registries that contain data extracted or abstracted (whether in whole or in part) from JHM medical records.

There are broadly three types of registries, albeit with considerable overlap:

1. Clinical registries required by regulation or national/international standards, such as registries for tumor, trauma, cardiac surgery and interventional cardiology. Clinical registries often are used for research but their raison d'être is compliance with government regulation or other standards.
2. Research registries, which typically are investigator-, division- or department-sponsored databases, single-site or multi-center. These include all IRB-approved indexes (including curations or annotations) used for patient- or case-finding.
3. Quality improvement/quality assurance registries, which typically are created to monitor QI/QA issues or initiatives.

Many of these registries contain data on thousands of patients and providers and often contain high-risk PHI and involve medico-legal vulnerabilities. The risk from registries is much greater than that from individual clinical studies and the extent of consequent JHM reputational risk and financial damage is larger; in the event of data breach, notification, fines, and institutional costs exceed $150 per patient, which may be charged to the responsible department or division.

For all of these reasons, the Johns Hopkins Medicine Data Trust, the Vice-Dean for Clinical Research and the JHM IRBs are adopting data management standards for registries, in addition to existing data management standards for general research data.

Note that the Epic system offers robust registry capability and security architecture. Epic's registry capability is the preferred mechanism for creating registries.

II. DATA REGISTRY TECHNICAL STANDARDS

These standards apply to registries that are "ongoing," meaning having a projected lifespan >2 years and having periodic updates or additions (as opposed to a static one-time data extract), with or without longitudinal follow up, and that are standalone systems external to Epic. These standards do **not** apply to repositories that contain data only on consented patients in a clinical study for which the protocol (including all future uses of data) was fully pre-specified at the time of IRB approval; to clinical reporting systems that put results into Epic; to operational data repositories; to data collections (e.g. Excel

spreadsheets) used for manual entry (e.g. via a web interface) to external registries; and to registries that are components of the Epic system. The standards apply to clinical research databases that are used for future research without a pre-specified protocol associated consent. As used in this guidance, the term “registry” or “registries” applies to clinical, research and QA/QI registries, unless specifically qualified.

1. Registries shall store their data in one of the following systems:
    a. An MS SQL Server, housed in an enterprise data center administered by IT@JH, behind a red zone firewall, and accessible to monitoring by the IT@JH enterprise security team;
    b. Other systems specifically approved for registry storage by the Research Data Subcouncil or Clinical and Quality Data Subcouncil of the JHM Data Trust.
    c. For clarity, some corollaries of the requirements above:
        i. Registries shall not store data in divisional or departmental servers or workstations.
        ii. Registries shall not store raw data (data that contains HIPAA “facial” or direct identifiers, as opposed to de-identified analytic files or HIPAA limited datasets) in non-SQL systems, such as Filemaker Pro, MS Excel, MS Access, and SAS or STATA data files. Without special provisions, such systems allow bulk query or file copying without SQL logging and protection. HIPAA identifiers are listed at http://www.hopkinsmedicine.org/institutional_review_board/hipaa_research/limited_data_set.html
2. All registry databases shall use JHED/Active Directory authentication and authorization and shall require Multi-Factor Authentication for administrative access and ad hoc/bulk query access to data containing HIPAA identifiers.
3. All registry databases shall be supported by a Database Administrator (DBA) with a reporting line up to IT@JH, who shall be responsible for data security.
4. Registries shall not store identifiable full-text documents (such as operative notes, discharge summaries, procedure notes, radiology reports and pathology reports) from the electronic health record except as required for operational purposes. Registries may store pointers to clinical documents, images, or data.
   Text repositories may be created by Precision Medicine de-identification processes. Requests for identifiable text repositories must be reviewed and approved by the Data Trust Research Data Subcouncil or Clinical and Quality Data Subcouncil.
5. Registry tables or files containing HIPAA identifiers (described in the link above), such as patient name and MRN, shall be logged. All registry extracts containing PHI shall be logged and retained for at least 2 years. Once extracted, analytic files without patient identifiers do not require logging.
6. For data security and concurrency reasons, registries shall not contain unneeded patient identifiers such as SSN, HICN, street addresses, phone numbers, email addresses or telephone numbers. (Typically data needed for follow up, such as SSN for death registry queries or addresses for follow up contact, are best obtained as one-time queries from enterprise data sources.)
7. Registries by definition are not completely de-identifiable--details in even nominally de-identified records often are recognizable to clinical staff--so registries cannot use a self-service export model. Patient-level data extracts shall be prepared by Data Trust Analytic Teams, with copies of each extract logged and retained in a data-archiving system.
8. Direct ad hoc access to raw data tables containing PHI by investigators or analysts shall be minimized to the extent possible, and shall be logged. These logging requirements do not apply to HIPAA limited or de-identified datasets, dashboards or aggregate queries (counts).
9. The Data Trust shall maintain an inventory of all JHM registries. To facilitate this process, all registries shall provide or update registry details bi-annually to the Data Trust.
10. Case-by-case exceptions to any part of this guidance require a written application and written approval from the Data Trust Research Data Subcouncil or Clinical and Quality Data Subcouncil.
11. Registry data access for any research purposes (including access to clinical, research and QA/QI registries) requires study-specific IRB approval. While a registry itself may have IRB approval, this does not imply umbrella approval for derivative or unspecified studies.

III. DISSEMINATION

These Guidelines and any updates will be available on the DTC website and on Hopkins Policy and Document Library online.

IV. SUPPORTIVE INFORMATION

References:

- Johns Hopkins Medicine Data Trust Policy

Sponsor:

- Data Trust Council

Developer(s):

- Data Trust Privacy and Security Subcouncil
- Data Trust Research Data Subcouncil
- Data Trust Data Stewardship Subcouncil