Technical, Regulatory and Structural Aspects of the ITMIG Database

Summary of steps to participate in the ITMIG Database (DB)

1. Register as a member of the ITMIG DB and obtain the security clearance. Go to https://ccehub.org/register/, and follow the directions. Helpful details to guide you through the process are provided in the document "Gaining Access to the ITMIG Databases", available at https://ccehub.org/itmig under the link Click here for Access Instructions.
2. Sign or have your institution sign the Data Use Agreement (DUA) between you or your institution and ITMIG. This gives ITMIG the right to receive the data, to store it in the database, to completely de-identify it (i.e. convert dates to intervals), and to make completely de-identified data from all contributors around the world able to be combined and used for any ITMIG approved research proposals.
3. Return the Data Use Agreement to Alberto Antonicelli, MD, ITMIG Database Manager, at alberto.antonicelli@yale.edu or fax 203-737-2167.
4. In the US, neither patient consent nor a research protocol is required for abstraction and submission of limited dataset (LDS, i.e. containing no patient identifiers but containing dates). However, an IRB review and waiver is required to access and review patient records for the purpose of abstraction of a LDS. Contributors in other countries must follow policies and procedure in place in their country, if these are different than those in the US.
5. Provide data to the ITMIG DB (link https://ccehub.org/itmig). No patient identifying information is allowed (except dates). Each patient will be assigned a number. No patient consent or IRB approval is necessary for data submission involving such a LDS.

Overview of ITMIG Database (DB) structure

Structure: The ITMIG DB involves only what is known as a limited dataset (LDS). This means it does not contain any patient identifiers except dates (e.g. date of diagnosis, treatment, birth, and death). This is considered to be low risk for potential disclosure of public health information (PHI), and is subject within the US to very few limitations on data sharing (defined in: http://privacyruleandresearch.nih.gov/pr_08.asp)

ITMIG assumes responsibility for the LDS. ITMIG may contract with another entity (e.g. HUBzero) to house, maintain, aggregate and fully de-identify the data, and ensures that such entities are fully compliant with HIPAA security and privacy regulations and meet all applicable regulations and safeguard requirements (outlined here https://hubzero.org/groups/itmig_hipaa_safeguards/wiki/).

Each contributing institution has unrestricted access to its own data. Such use of an institution's own data is governed by the laws and policies applicable at that institution and is the responsibility of that institution.

The primary purpose of the ITMIG DB is to improve outcomes for patients through collaborative research, which will involve completely de-identified data (no dates). Completely de-identified data carries no risk of privacy violation, and can be used for research is without patient authorization. No IRB approval for completely de-identified data is needed, although an IRB review and waiver for documentation is common practice.

The process for gaining access for research to this de-identified data is as follows: A request from any person or institution eligible for access (as defined in the Database policies) must be approved by the ITMIG DB (and must include IRB waiver). The requested data will be provided only as completely de-identified data for use as outlined in the ITMIG DB policies. ITMIG assumes responsibility that release of the data is in accordance with US policies and laws that apply. It is the responsibility of an individual investigator to adhere to any local restriction regarding research using deidentified data, should these exist within the investigators country or region.

For ITMIG to function in its role of facilitating appropriate collaborative research, each institution contributing data must grant ITMIG the right to permit use of the data for research as defined in the ITMIG DB policies. ITMIG assumed responsibility for assuring that these policies are adhered to, and that use of the

data is in accordance with US laws in effect, that the research is appropriate and that the data released is completely de-identified. The Data Use Agreement (DUA) allows ITMIG to perform these functions.

Details of the ITMIG Database

Use of Data:

The limited dataset (LDS, i.e. containing dates) is available to the submitting institution without restrictions. It is the responsibility of each institution that its use of its own data is in accordance with laws and policies in effect at the respective institution.

Completely de-identified data (i.e .containing no personal identifiers or dates) can be made available for research purposes, as governed by the access rules of ITMIG (see below) and in accordance with US laws pertaining to de-identified data.

Access for Research:

Only completely de-identified data will be available for research. Completely de-identified data is not considered "human subjects research" (see ….) and therefore its use for research is in accordance with international laws without patient authorization or IRB approval.

A participating institution has access to its own data in a completely de-identified form for research purposes without restriction; it is the responsibility of the institution to ensure that the such use is in accordance with the laws and policies in effect at the institution. A participating organization (e.g. ESTS) has access to its own data in a completely de-identified form for research purposes without restriction; it is the responsibility of the organization to ensure that such use is in accordance with the laws and policies that apply to the organization and the participating institutions of the organization.

Research involving the entire DB or a portion beyond an institution's or organization's own data must be approved by ITMIG in accordance with its policies for such research. ITMIG assumes responsibility for assuring that the data being used for research as described in this paragraph is completely de-identified.

Regulations Pertaining to the ITMIG DB

Summary: *The ITMIG database is structured in full accordance with US laws* governing the security and privacy of health-related data involving human beings (see Security Safeguard Assessment for the ITMIG Database and References and Information Links for more information). According to these laws, under the structure and operations of the ITMIG database, *patient authorization to participate is not required, and institutional IRB approval to submit data is not required*.

Background: HIPAA is the acronym for the Health Insurance Portability and Accountability Act, in effect in the US since 1996. The "Privacy Rule" is a regulation under HIPAA that restricts the use and disclosure of "Protected Health Information" (PHI) by "Covered Entities." A "Covered Entity" under HIPAA includes Hospitals, physicians and other health care providers – therefore participants in the ITMIG DB are included and fall under this regulation. The "Common Rule" is the federal regulatory standard of ethics to which any government-funded research in the US is held. HIPAA does not pertain to non-US participants of the ITMIG DB.

The ITMIG DB is designed to adhere to the principal Data Access Rule:"hospitals have access to the database to contribute and explore only their own patient data"

No Need for Institutional IRB permission to submit Data to the ITMIG database:
The HIPAA rules do not require each institution that submits data to a multisite registry that may be used for research purposes to obtain separate approval from its own IRB, provided that one IRB has approved the registry (which we have).[1] *Thus, an institutional IRB approval to submit data is not required.*

HHS has stated (65 *Federal Register* 82692, December 28, 2000) that a covered entity's responsibility is to "obtain the documentation that *one* [emphasis added] IRB or privacy board has approved the alteration or waiver of Authorization." Consequently, the Privacy Rule allows a waiver or an alteration of Authorization obtained from a single IRB or Privacy Board to be used to obtain PHI in connection with a multisite project. However, HHS also recognizes that "covered entities may elect to require duplicate IRB or Privacy Board reviews before disclosing [PHI] to requesting researchers" (67 *Federal Register* 53232, August 14, 2002)".[1] Additional information on the Privacy Rule and IRBs can be found in an article entitled *Institutional Review Boards and the HIPAA Privacy Rule*.

Regulations governing potential research uses:
Note that an institution or organization conducting research on its own data, which is stored in the ITMIG database, must comply with regulations for conducting this research applicable at the institution or regions in which the research is done. Research involving a completely de-identified dataset and in which the researchers are completely barred from access to the code key is not considered "human subjects research" and does not require IRB approval. However if the researcher has potential access to the code key then local IRB approval much be obtained.[2]

Research involving completely de-identified data, and in which no interaction with research subjects occurs is considered to be NOT "human subjects research".[2]

"OHRP does not consider research involving **only** coded private information (or specimens) to involve human subjects as defined under 45 CFR 46.102(f) if the following conditions are both met:

1. the private information [was] not collected … through an interaction … with living individuals; and
2. the investigator(s) cannot readily ascertain the identity of the individual(s) to whom the coded private information or specimens pertain because, for example … the investigators and the holder of the key enter into an agreement prohibiting the release of the key to the investigators under any circumstances".[2]

Thus, research conducted under the structure of the ITMIG database does not require patient authorization or IRB approval from institutions contributing this data or the researcher involved.[2]

Patient Consent

"The Privacy Rule permits a covered entity, without obtaining an Authorization or documentation of a waiver or an alteration of Authorization, to use and disclose PHI included in a limited data set".[1]
Written Authorization from research participants is not needed "for research for which the use or disclosure of the PHI is permitted by the Privacy Rule".[3]
"The Privacy Rule permits covered entities to release data that have been de-identified without obtaining an Authorization and without further restrictions upon use or disclosure because de-identified data is not PHI and, therefore, not subject to the Privacy Rule".[3]
Thus patient consent is not needed under the structure of the ITMIG database (submission of a limited dataset).

Limited Data Sets
A covered entity may disclose PHI "if the information is released in the form of a limited data set, with certain identifiers removed, and with a data use agreement between the researcher and the covered entity".[3]
"Limited data sets may be used or disclosed only for public health, research, or health care operations purposes. … Before disclosing a limited data set to a researcher, a covered entity must enter into a data use agreement with the researcher, identifying the researcher as the recipient of the limited data set, establishing how the data may be used and disclosed by the recipient, and providing assurances that the data will be protected, among other requirements".[3] Additional information on limited data sets and data use agreements can be found in the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy*
A covered entity does not need to account for disclosures of PHI contained in a limited data set[3] (disclosure means "The release, transfer, access to, or divulging of information … outside the entity holding the information").
Thus, a signed Data Use Agreement between ITMIG and contributing institutions/individuals is needed before institutions or researchers can participate in the ITMIG database.

De-Identified Data
"So long as the health information is de-identified according to the Privacy Rule, the Privacy Rule does not apply to the database or to future uses and disclosures of de-identified data from the database".[3]
"The Privacy Rule permits a covered entity to retain … a code or other means of record re-identification" of the de-identified data.[3]

References
1. HIPPA Privacy Rule: information for Researchers. http://privacyruleandresearch.nih.gov/pr_08.asp
2. U.S. Department of Health & Human Services: Guidance on Research Involving Coded Private Information or Biological Specimens. http://www.hhs.gov/ohrp/policy/cdebiol.html
3. Research Repositories, Databases, and the HIPAA Privacy Rule
http://privacyruleandresearch.nih.gov/research_repositories.asp