PARTNERS HEALTHCARE

FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

Partners Research Data Management Requirements

Partners Research Compliance Office

February 15, 2018

Table of Contents

1. Introduction- Definitions and Key Concepts

The purpose of this document is to provide a framework for the research community of Partners HealthCare ("**Partners**") affiliated hospitals and institutions (each an "**Institution**") to manage research data, materials, and information in compliance with regulatory requirements, institutional policy, and sound scientific practice. The primary purpose is to set forth minimum standards to ensure **electronic and paper** research data, materials and information are accurately, reliably, and safely maintained. This document includes minimal information on management of tangible research materials, e.g., cell lines or mouse colonies. Detailed requirements for tangible research materials will be published at a future date in conjunction with hospital Environmental Health and Safety departments, the Partners Institutional Biosafety Office (PIBC), and hospital Institutional Animal Care and Use Committees (IACUC.)

As each research endeavor is different, not all requirements and best practices outlined in this document will apply to all electronic or paper research data, materials, and information. When determining which practices to adopt, Principal Investigators ("**PIs**"), Co-Investigators, researchers and their staff should keep in mind the specific types of research data, materials or information generated by their laboratories.

Definitions

The *Partners Research Information Ownership Policy* includes definitions of Research Data, Research Materials, Research Records, and Research Information applicable to all research conducted at Partners institutions. PIs should review these definitions, in addition to the *Partners Guidelines on Retention of Research Data, Materials and Records*, when developing data management plans.

For the purposes of this guidance, Research Data are any, and all, electronic or paper data and information created or collected in the process of performing research.

Research Data Ownership

Research Data, including Research Materials, Information and Records, arising from research conducted at a Partners institution using institutional space and/or resources or otherwise conducted under the auspices of a Partners institution are owned and controlled by that institution. This includes research conducted at any site (including off-site) by Partners investigators working in their Partners institutional capacity.

PIs, as the "data responsible party," along with their staff, are responsible for ensuring the Research Data, materials, and documents they collect are organized, stored, and transported securely in keeping with Partners and hospital policies and guidelines for recordkeeping, data management, data security, and retention. Tangible research materials (e.g., cell lines, chemical agents) should be stored in appropriate hospital facilities (e.g., freezers, incubators, cold or warm rooms); electronic Research Data

or information must be stored on appropriate hospital devices (e.g., desktop computers, laptop computers, portable hard drives, or flash drives.) Whenever possible and allowable by regulation and/or institutional policy, paper Research Data or records may be scanned and stored electronically.

Data Classification

Partners categorizes data into three broad areas

- **Public Data**
- **Institutional Data**, or
- **Confidential Data**.

Consideration of the lab's Research Data classification(s) and the applicable regulations and institutional policies triggered by categorization is a necessary precursor when formulating the lab or research group's data management plan. Briefly, Research Data may be categorized as

> **Public Data**: Data created for public consumption such as published data or data that have been de-identified in accordance with HIPAA and Partners IRB standards and classified as public by Partners Information Security and Privacy.
>
> **Institutional Data**: Data not subject to a regulatory or contractual confidentiality requirement, but Partners has decided to keep the data private for business reasons. For example, patent applications, draft research papers, or non-human subjects research study data.
>
> **Confidential Data**: Any regulated, contractually, or identifiable protected data, including Limited Data Sets ("**LDS**"), are considered confidential.

For more information on data classification and the security requirements associated with these categories, please consult EISS8.1c IT Asset Management Standards for Data Classification.

The Data Life Cycle

Data associated with a research project follow a cycle from collection to destruction that includes analysis, use, sharing, storage, and archiving (the "Data Life Cycle"). Each stage of the Data Life Cycle involves unique challenges of integrity and security that should be addressed by the research team.

Data Security

Data security is a broad concept that includes measures to keep Research Data safe from intentional and unintentional acts that may damage or destroy data or inappropriate release or access. How Research Data are kept secure depends on the type of data being considered.

- Electronic-based data often require physical protections which prevent the data from being broken or damaged by physical elements and programming protections (encryption) which limit access to data and track any changes that are made to an electronic record (audit trail).

- Paper-based data may be easier to track for intentional changes (i.e., fabrication or falsification of data), but are challenging to store safely for long periods of time.

- Research materials (tangible data), such as genetic elements, mouse colonies, or frozen biological specimens present challenges in demonstrating the authenticity of the specimen, as well as protecting its integrity during long-term storage.

Data Integrity

Data integrity is a measure of how accurately and reliably Research Data reflect the study's research activities. Researchers may be called upon to demonstrate the integrity of their Research Data to government agencies, sponsors, and publishers, as well as to Institutional officials during a Research Misconduct proceeding. By considering how Research Data are collected, stored, and analyzed, researchers can build data integrity checks into each stage of the Data Life Cycle.

Research Misconduct

Research Misconduct is defined by federal law as fabrication, falsification or plagiarism of Research Data in proposing, performing, or reviewing research or in reporting research results.[1] In compliance with the federal regulations, Partners has developed institutional policies and procedures for investigating instances of alleged misconduct. These policies apply to all research at Partners Institutions, irrespective of funding source. Because Research Data are at the center of all research misconduct proceedings, the strength or weakness of a research group's data record keeping practices will have a major impact on research misconduct cases.

For more information on Research Misconduct, please consult the Partners Policy and Procedures for Handling Allegations of Research Misconduct or the federal regulations on Research Misconduct. To report an allegation of fabrication, falsification, or plagiarism, please contact your Institution's Research Integrity Officer (RIO).

2. Data Management Plans

A Data Management Plan ("**DMP**") is a description of how Research Data will be collected, maintained, shared, retained, and destroyed throughout a research project.

The project's PI is responsible for

- **Creating the DMP before the start of a new research project;**
- **Including a copy in the project's records; and**
- **Making the DMP accessible to all participants**

[1] Public Health Service Policies on Research Misconduct, Final Rule; 42 CFR §93.103

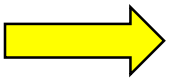
Certain research sponsors, such as the NSF, require a DMP as part of their applications for funding. Other agencies, such as the NIH, routinely ask grantees to address specific data management elements such as data sharing and data security. Research staff who want to gain access to large external data sets for research purposes are often asked to submit a DMP before obtaining access to the data. In these situations, the PI should contact the sponsor or data owner (individual or institution from whom the Research Data were obtained) for specific DMP requirements.

In addition to sponsor-mandated DMP elements, the DMP includes the following:

- **Project Description** – Project title, funding source, staff working on the project, start and end date of the project, and a short description of the research taking place.
- **Form of Data Collected** – Will the Research Data be pictures, images, measurements, electronic files, written records, electronic health record data (e.g., RPDR), or a combination of these? Will the Research Data include patient samples, biological samples, or genetic elements? Describes all the forms of Research Data you will collect.
- **Type of Data Collected** – Are the Research Data de-identified? A Limited Data Set (LDS)? Will the Research Data contain identifiable health information or other confidential information?
- **Data Sharing** – Will you share your Research Data? With whom? Are there any sponsor or institutional limitations on data sharing that require a Data Use Agreement (DUA), Material Transfer Agreement (MTA), or other contractual arrangement? If the study involves consented subjects, does the informed consent document limit data sharing?
- **Short Term Storage** – How will the Research Data be stored during the time the project is active? How many copies of the Research Data will you store? Where will these copies be physically located? Who can access, analyze, or add to the data set?
- **Long Term Storage** – How long will you store Research Data after the project has been completed? If the Research Data are electronic, what file type will you use for storage? How many copies will you keep and who will have access to these copies?
- **Security** – How will you prevent Research Data from being lost, stolen, altered or accessed inappropriately? What would happen if there was a disaster in the building?

There are many useful tools to assist PIs in the creation of a DMP. The University of California Curation Center has created DMPTool, which allows researchers to create a DMP based on sponsor requirements. The United Kingdom's Digital Curation Center also provides free web-based tools for creating DMPs. In addition, MIT offers a great deal of practical information on how to plan for safeguarding research data throughout the lifecycle.

On occasion, it may be difficult to determine whether a new project or a new grant requires its own DMP, especially if the project/grant is closely-related to ongoing work in the research group/lab. In these situations, we strongly recommend that PIs err on the side of caution and create a separate DMP for the new project. However, if the PI determines creating a new DMP is unnecessary, s/he must revise the existing DMP to reflect inclusion of the new project /grant and make necessary changes in all DMP components, e.g., roles and responsibilities; staff roster; access; security; storage requirements; and SOPs. The PI is also responsible for including a copy of the revised DMP in the records of both projects/grants and for making the revised DMP accessible to all members of the lab/research group.



If as of the publication date of this document, an ongoing study does not have a DMP, the PI is required to develop a DMP as soon as reasonably possible, but not later than the compliance date of May 15, 2018, include a copy in the project's records, and make the it accessible to all project/grant(s) participants.

2.1 Roles and Responsibilities

All members of a research team, both as data generators and users, have a role in the proper management of Research Data. An important part of the DMP is identification of roles and responsibilities and data use and sharing rights of all members of the research team. Responsibility for the overall management of the study resides with the PI who is responsible for providing data management training to his/her research staff, in addition to setting clear expectations of roles and responsibilities. The PI may delegate day-to-day data management responsibility to another member of the study team but ultimately the PI is accountable for compliance with regulations and sponsor and institutional policies. The following is a general description of roles and responsibilities associated with data management. [2]

[2] Based on tables included in Guidelines for Responsible Data Management in Scientific Research, Office of Research Integrity, US Department of Health and Human Services. http://ori.hhs.gov/images/ddblock/data.pdf AND, Lyon, Liz; Dealing with Data: Roles, Rights and Responsibilities, UKOLN, June 2007

Research Team	Roles & Responsibilities	Accountable to
Principal Investigator	• Initiates research studies, designs and implements research protocols. • Requests funding from research sponsors. • Responsible to the Institution, Sponsors, and regulatory entities for conduct of the research study. • Writes, publishes, and otherwise disseminates research findings. • Creates and manages the environment in which the research activity takes place. • Provides oversight, mentorship, and guidance to research staff.	• The Institution • The Sponsor • Regulatory Groups • Government Agencies
Project Manager	• Manages day to day operations of the research group. • Creates policies and procedures to ensure compliance with the research protocol, laboratory policies, and regulatory requirements. • At PI's direction, works with sponsor, regulatory agency, or institution on data issues.	• Principal Investigator • Institution • Regulatory Groups
Clinical Research Coordinator Research Assistant Technical Research Assistant	• Carries out the protocol or performs experiments as directed by the PI, Project Manager or another research staff (e.g., Co-Investigator). • Records research activities and results per established practices of the research group.	• Project Manager/Co-Investigator • Principal Investigator • Institution
Institution	• Provides infrastructure to allow the PI to maintain research data securely and in compliance with sponsor requirements and applicable regulations. • Has an obligation to comply with all applicable regulations.	• Sponsor • Regulatory groups • Governmental Agencies • Legal requirements

2.2 Data Collection

Detailed record keeping has always been a crucial scientific tool. Scientists have relied primarily on lab notebooks to chronicle the progress of scientific inquiry and support findings when presented to the larger scientific community. The information recorded in lab notebooks or other recordkeeping media

allows other scientists to replicate experimental conditions and confirm or deny research findings. When maintained appropriately, paper lab notebooks can provide proof of reduction to practice in intellectual property disputes and resolve allegations of data fabrication or falsification.

Record Keeping Systems

Paper-Based Record Keeping

Historically scientists have relied on paper-based lab notebooks to document their hypotheses, experiments, and analysis. This information ensures results can be reproduced at any time in the future and there are traceable records. Entries are written in real time as they occur and not from memory later. Paper lab notebooks offer easy and flexible options for maintaining the security and integrity of the research record.

Paper-based lab notebooks must always be bound with pages sequentially numbered, so that missing pages are apparent to the reader, and include the following content:

- **Table of Contents:** A listing of each experiment performed for a specific project's aim or hypothesis
- **Materials Used:** Include chemicals, reagents, cell lines or specimens, for projects that are computational or informatics driven include software programs used.
- **Methods Used:** A description of the steps taken to complete the experiment such that another scientist could replicate the experiment
- **Results**: The raw Research data resulting from the study
- **Analysis and findings**: Any steps taken to clean, organize, and analyze the Research Data and any conclusions reached

Entries must be written in ink with mistakes crossed out and initialed. Each page in the notebook must be completely-filled before a new page is started. If necessary, blank space on a page should be blocked off with an X. Each entry in the research notebook should include the minimum content elements described above. Include sketches and diagrams in the notebook with an explanation. Permanently attach source data, e.g., photos, gels, and other output, whenever possible or, at a minimum, indicate where these are stored in hard copy or electronically. All entries must be in English.

The PI or his/her designee is responsible for reviewing laboratory notebooks on a regular basis. When a laboratory notebook is used to support a patent application, it is common practice for a witness to sign and date the notebook to confirm its accuracy as a record.

Electronic-Based Record Keeping

Many research groups generate electronic data, files, and images as source data that must be referenced or integrated with a paper-based lab notebook for recordkeeping. **It is important to**

remember that many popular applications, such as Microsoft Excel or Word, do not have the necessary access controls to prevent intentional or unintentional changes to data, or the audit trails to identify changes made to a data set over time. Many of these challenges can be overcome by cross-referencing electronic source data with paper lab notebooks, saving multiple copies of electronic source data in read-only formats, and storing the electronic source data in a location that only the PI can directly access. Regardless of how electronic source data are stored, they must include the same content, security, and integrity controls applicable to paper records.

Electronic Laboratory Notebooks (ELN)

ELNs are more than the contents of a written notebook captured in a word processing program. ELNs are fully integrated systems that can capture large amounts of electronic data from measuring devices or research machinery programmatically while also permitting the user to enter experimental data manually. ELNs can be searched and shared, in whole or in part, much more efficiently than traditional laboratory notebooks. Audit trails and permission levels protect data integrity throughout the Data Life Cycle. ELNs also provide a mechanism for central storage of laboratory records and protect against accidental loss or disclosure. Like paper lab notebooks, the ELN should include the equivalent of a table of contents and record the project's aim or hypothesis, materials used, methods used, results (raw data), and findings with all entries in English.

Partners Research IS Computing supports LabArchives, an ELN system that is available to Partners research groups at no cost. PIs can establish a LabArchives account with their Partners user name and password. For additional information, login at: rc.partners.org/eln.

DMP/Data Requirements Audit Plan

Within 12 months of publication of this document, Partners Internal Audit, in conjunction with hospital Research Compliance, will initiate a pro-active, not-for-cause audit program focused on compliance with DMP and related Partners data requirements outlined in this document. A sample of research projects/labs from each hospital will be selected for audit. Audit reports will be presented to the PI, Chief, SVP for Research/equivalent position, and hospital and Partners Research Compliance. If there are audit findings, hospital Research Compliance will work with the PI to develop and monitor a Corrective Action Plan (CAP) based on the findings and will notify the Chief, SVP and Partners Research Compliance when CAP requirements have been met.

As needed, upon request of the hospital SVP for Research/equivalent position, Partners Internal Audit, in conjunction with hospital Research Compliance, will conduct for-cause audits. Audit reports will be presented to the PI, Chief, SVP for Research/equivalent position, and hospital and Partners Research Compliance. Hospital Research Compliance will work with the PI to develop and monitor a CAP based on the findings and notify the Chief, SVP for Research/equivalent position and Partners Research Compliance when CAP requirements have been completed.

Depending on the seriousness of the audit findings, the CAP may include the possibility of additional audits in the future and sanctions and/or other disciplinary actions as required by the applicable Partners policies.

3. Data Storage

Appropriate data storage for a research project often involves short-term, long-term, and back-up components. When the study is active and data collection and analysis are ongoing, short-term storage solutions often focus on accessibility and portability. Later, when the study is complete, long-term storage may favor file formats that are more likely to stand the test of time and protect the integrity of the dataset. Backing-up data and storing it in a secure location that is physically removed from other copies of the data are crucial to protecting the valuable investment that has been made in any research activity. Research IS Computing has a host of services for long and short-term storage of data, as well as ways to back-up small and large data sets securely and efficiently.

Back Up Copies

At least one back-up copy of all Research Data should be maintained throughout the project's Data Life Cycle. The PI, as the "data responsible party," is responsible for developing and maintaining procedures for how back-up copies will be created, how often, in what format, and where the copies will be stored. For paper-based records keeping a back-up may involve photocopying, scanning, or taking a digital picture of a printed page. Some paper notebooks have built in carbon copy pages to allow copies to be created with the original record. Regardless of format, back-up copies may not be stored with original Research Data.

When keeping back-up copies of electronic-based records, it is important to consider how long the records will be maintained and whether there are any special protections, such as confidentiality, that should be applied to the copy. The safest place for short-term storage of electronic-based data is an encrypted external hard drive. Research IS Computing can provide PIs with acceptable Partners options. Portable devices, such as flash-drives and disks, are not designed for long-term storage. They lose integrity over time and may not be used for Research Data generated under Partners research projects. Computer hard drives can also break down over time. The safest place for long-term storage of electronic-based Research Data is secure network storage. As file formats tend to change over time, it is best to store Research Data in a standard form, for example, as a PDF or text file.

Storage Logs

Storage logs are required for all Research Data stored in a lab or research group, including, but not limited to, paper-based Research Information and electronic-based Research Information, and Research Materials, i.e., research specimens, frozen stocks, and cell lines. Storage logs should include additional metadata about the research record that would help others understand the context in which

it was created or saved. The type of metadata recorded in a storage log will vary by project. The following are some examples of metadata to include in a storage log:

- IRB Protocol number
- Grant Number or Proposal Number
- Project name
- Whether the data are public, institutional or confidential, or otherwise protected from disclosure
- A description of what an electronic file contains
- The original of a cell line; a description of the plasmid or vector used in the study

In addition to storage logs, Partners policy requires staff to maintain a log of all electronic devices, both personal and owned by the hospital/Partners, which store Research Data that contain protected health information ("**PHI**")[3]. This log must identify instances when such PHI is removed or copied to another computer or portable device, including but not limited to, CDs and flash drives. Regardless of the type of Research Data, every laboratory is required to maintain a list of the desktop computers, laptop computers, and other mobile devices (including mobile phones and tablets, portable hard drives and flash drives, and any other portable device that can be used to store data) that contain Research Data, and the type of protections employed on each device.

File-Naming Conventions

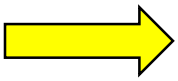
Research Information files (e.g., records and Research Data) should be named in a consistent way that will allow future investigators or hospital staff to identify what the record or file contains. For example, the file name could reference the project title, grant number, or a specific experiment within the project. It could also include the initials of the person completing the experiment, or the date it was started. Starting a common naming convention for each project will help properly identify records that will be stored long-term and/or that are part of a large study and should be recorded in the DMP. It is important to remember when establishing a file-naming convention, not to include PHI or HIPAA identifiers in file names.

4. Data Sharing

Research sponsors, funding agencies, scientific journals, and other groups are placing greater emphasis on sharing data amongst research groups. Data entering or leaving a Partners Institution must be accompanied by an agreement outlining how the data will be used, protected, and maintained, e.g., through a formal Data Use Agreement (DUA) negotiated by a Partners office or a template letter agreement signed by the sharing and receiving PIs. Incoming and outgoing data with information on human subjects or PHI require IRB review. Unless otherwise stated in the incoming DUA, IRB approval

[3] Partners Healthcare Inc. Information Systems Security Policy, Accountability of Electronic Media (PH-539)

must be received before the Partners PI accepts the data. For outgoing data with information on human subjects or PHI, IRB approval must be received prior to DUA execution.



The Partners Data & Tissue Sharing Committee (PDTSC) was established in 2015 to evaluate requests to disclose or provide access to Partners clinical and research data and tissue to external parties and is charged with ensuring that clinical data and tissue sharing with external parties (both non-profit and for-profit organizations) is consistent with the charitable mission of Partners and its affiliated hospitals.

The PDTSC acts as a data and tissue steward and facilitates consistent and responsible sharing of Partners clinical and research data and tissue assets to promote research and improve patient care. Not all data sharing situations are subject to PDTSC review. When and how to obtain PDTSC approval is addressed later in this document. When PDTSC review is required, the Committee alone is empowered to determine whether the data and/or tissue sharing arrangement may move forward.

The sections below provide an overview of the common Partners data sharing scenarios. They include general information related to incoming and outgoing research data, institutional requirements, PI responsibilities, and Partners offices involved in the process.

Where to go/What to do

Incoming and Outgoing DUAs from/to Non-Profit Institutions, Foundations, and/or Government Entities

An Incoming Data Use Agreement (DUA) is an agreement that allows Partners institutions/investigators to access or obtain patient/subject data from an outside party for use in research. An Outgoing DUA is an agreement that allows a PI to share patient/subject data with an outside party for use in research. The data may be PHI, a LDS, or de-identified within the meaning of HIPAA. The outside party may be a non-profit institution or entity, government agency, or other public entity. Data may be shared as part of an ongoing collaboration between the parties or for independent research by the outside party. When an ongoing collaboration is planned, terms related to data sharing and data use may be incorporated in a research collaboration agreement thereby eliminating the need for a separate data use agreement.

Review and negotiation of an incoming or outgoing DUA from/to a non-profit institution, government agency, or other public entity is handled by Partners Research Management. Requests should be submitted through the Insight 4.0 Agreements module and include the following information:

- List of HIPAA identifiers to be sent/received;
- IRB protocol number and/or written IRB exemption determination;
- DUA from outside party, as applicable;
- Outside party entity name, PI name and administrative contact information;
- Purpose of data exchange;
- Relevant background information; and
- Whether DUA is related to an existing award (include Insight agreement number) or a new project.

Upon receipt of an executed incoming DUA, the PI is responsible for reviewing the terms to identify any requirements for security, access, sharing, or retention/destruction, and incorporating them into the project's DMP, and managing the data accordingly.

Depending on the DUA terms, the institution may not have the authority to approve secondary uses of data received from another institution or organization. If you want to share data received from another institution with another Partners PI, before sharing the data, contact Partners Research Management (bwhsubs@partners.org; mghsubs@partners.org; mclsubcontracts@partners.org; SRHGC@partners.org) to determine if the transfer is permitted and which documents are required for the data transfer.

Where to go/What to do

DUAs Related to Industry-Sponsored Clinical Trials

The Partners Clinical Trials Office (CTO) is responsible for developing, negotiating and executing incoming and outgoing data use/transfer/sharing agreements (also known as DUAs) with industry that may contain identifiable human subject data or that are related to clinical research.

Incoming and outgoing DUAs should be submitted to the CTO through the Insight Agreement module submission process. The DUA must:

- Specifically define or describe the data/dataset that the Partners institution/investigator is receiving from or sending to the industry sponsor;
- Specify all of the data elements or a description of the data elements;
- Specify scope of data use; and
- In order to determine the level of identifiability of the patients to whom the data pertain, the DUA must also include a designation as PHI, de-identified within the meaning of HIPAA, or a Limited Data Set (LDS), also within the meaning of HIPAA,

At various stages throughout the DUA review process, the Investigator is responsible for confirming the following:

- The data are accurate and complete;
- Data have been de-identified within the meaning of HIPAA;
- Data contemplated as part of the research engagement are limited to the minimum necessary to meet the study objectives;
- Appropriate subject consent has been obtained for data sharing (with IRB confirmation); and
- Notification to CTO if there are any other agreements related to the research under the proposed DUA.

When negotiating a DUA for incoming data, CTO ensures the de-identified data are de-identified within the meaning of HIPAA privacy regulations; that a LDS is an LDS within the meaning of HIPAA privacy regulations; specifies such in the DUA; and obtains written representation from the industry sponsor that it is in compliance concerning data provided and has the authority and permission to provide the data to Partners.

On occasion before making a determination whether the institution/investigator has the right to share the data with an industry sponsor and signing a DUA, the CTO will refer the industry data sharing request to the Partners Clinical Data and Tissue Sharing Committee (PDTSC) for review and approval under the following conditions:

- The request is to share de-identified data or images that could potentially be included in a commercial product or development, validation of a pre-existing software soslution/tool, or development of a new product;
- The request includes secondary use of data;
- Data request is outside the original scope of work; or
- The request is for a large amount of data.

If the data sharing request is referred to the PDTSC, CTO and PDTSC staff will work with the Investigator to identify materials required for PDTSC review.

Where to go/What to do

DUAs Related to Industry-Sponsored Basic Research

DUAs related to basic (bench) research with industry allow a Partners institution/investigator to access, obtain or share data with industry (for-profit) collaborators. In all instances the investigator must consult with the IRB to determine if IRB review will be required for the activity.

Partners Innovation Transactional Affairs Group (TAG) is responsible for developing, negotiating and executing data use/transfer/sharing agreements (also knowns as DUAs) with industry for basic research or human data the IRB has determined to be de-identified. Incoming and outgoing DUAs should be submitted to TAG through the Insight Agreement module submission process.

TAG is responsible for the following:

- Ensuring de-identified data are de-identified and/or constitute a Limited Data Set (LDS) within the meaning of HIPAA;
- Use is limited to the scope of the project; and
- Confirming with the industry sponsor that data will not be sold or used for marketing purposes.

At various stages throughout the DUA review process, the Investigator is responsible for confirming the following:

- The data are accurate and complete;
- Data have been de-identified within the meaning of HIPAA;
- The data contemplated as part of the data or tissue sharing engagement is limited to the minimum necessary to meet projective objectives/scope;
- Appropriate subject consent has been obtained for data sharing (with IRB confirmation); and
- Notification to TAG if there are any other agreements related to the research under the proposed DUA.

On occasion before making a determination the investigator/institution has the right to share data with industry and prior to signing the DUA or MTA, TAG may refer the request to the PDTSC for review and approval under the following conditions:

For a DUA:

- Data sharing request intends to leverage data solely as part of a product development or commercial validation;
- Scope of use includes secondary use to leverage data or derived data as part of product development, validation, study, or other commerical activities;
- The request is to share de-identified data fields beyond disease status or basic demographic information;
- The costs to collect and transmit data have not been factored into payment or financial considerations;
- Insights or results from study are not being shared back with Partners or affiliated hospital/institution;
- Data request is outside the original scope of work; or
- The request is for a significant amount of data.

For a MTA:

- Tissue sharing request intends to leverage tissue solely as part of a product development or commercial validation study;
- Tissue sharing request includes more than the following de-identified data fields:
  - Tissue type (e.g., blood)
  - Disease status (e.g., healthy, lung cancer)
  - Demographic information (e.g., gender, age group)
- Tissue samples will be used to obtain whole genome or exome data;
- Tissue samples are limited to patient specimens that may be important for future clinical and/or research use;
- The cost to collect and transmit samples have not been factored into payment or financial considerations;
- Insights or results from study will not be shared with Partners or affiliated hospital;
- Scope of use includes secondary use to leverage tissue or derived data as part of product development, validation study or other commercial activities; or
- Tissue request is outside the original scope of work.

If the data sharing request is referred to the PDTSC, TAG and PDTSC staff will work with the Investigator to identify materials required for PDTSC review and approval.

Where to go/What to do

Incoming Data: Secondary Use

It is not uncommon for a DUA or other research agreement for data received from an outside party to prohibit the investigator/institution from using the data for secondary use or distributing the data to another party without approval from the providing institution/entity. If you wish to share data received from another institution with a Partners PI, this transfer must be reviewed to see if the transfer is permitted and which documents may be necessary for the transfer to occur. Questions should be referred to the Partners office that neogtiated/executed the agreement with the outside party.

Where to go/What to do

Incoming and Outgoing DUAs: Limited Data Set (LDS)

A Limited Data Set (LDS) is PHI from which most HIPAA direct identifiers, such as name and medical record number, have been removed, but which may contain a limited set of identifiers, such as dates and/or limited geographic and demographic information. Partners may use or disclose a LDS as

permitted by the HIPAA Privacy Rule, including for purposes of research, public health, and health care operations if certain administrative safeguards are in place.

Incoming LDS: On occasion the institution providing the LDS to a Partners investigator/institution may not require a DUA for the transfer. The Partners PI may not accept the data without a DUA and should refer any questions to the appropriate office: Research Management, CTO, or TAG.

Upon receipt of incoming data, the Partners PI is responsible for reviewing the DUA to determine whether there are special requirements for security, access, sharing, or retention/destruction incorporating them into the project's DMP; and managing the data accordingly.

Outgoing LDS: Prior to sharing a LDS with an external collaborator, the PI must first obtain IRB approval for the transfer. In accordance with the Partners Limited Data Set policy, once IRB approval has been obtained, the PI may use the outgoing DUA template included within the policy. The DUA template may be issued and signed by the Partners PI provided no changes have been made to the terms.

Where to go/What to do

Partners Data & Tissue Sharing Committee (PDTSC)

As stated at the beginning of this section, the PDTSC was established to evaluate requests to

- Disclose or provide access to Partners clinical and research data and tissue to external parties;
- Ensure data sharing with external parties (non-profit and for-profit) is consistent with the charitable mission of Partners and its affiliated hospitals;
- Serve as a data and tissue steward; and
- Facilitate consistent and responsible data sharing to promote research and improve patient care.

Co-chaired by the Partners Chief Academic Officer and Chief Medical Officer, the PDTSC reviews data sharing requests referred to them by the Partners offices listed below.

- Partners Clinical Trial Office (CTO): DUAs related to industry-sponsored clinical trials
- Partners Innovation Transactional Affairs Group (TAG): DUAs related to industry-sponsored basic research.

Not all data sharing requests reviewed by CTO or TAG require PDTSC review; however, when PDTSC review is required, the PDTSC alone is empowered to determine whether the data and/or tissue sharing arrangement may move forward.

CTO will refer the data sharing (DUA) request to the PDTSC for review and approval under the following conditions:

- The request is to share de-identified data or images that could potentially be included in a commercial product or development, validation of a pre-existing software solution/tool, or development of a new product;
- The request includes secondary use of data;
- Data request is outside the original scope of work; or
- The request is for a large amount of data.

TAG will refer tissue (MTA) or data sharing (DUA) requests to the PDTSC for review and approval under the following conditions:

For a DUA:

- Data sharing request intends to leverage data solely as part of a product development or commercial validation;
- Scope of use includes secondary use to leverage data or derived data as part of product development, validation, study, or other commercial activities;
- The request is to share de-identified data fields beyond disease status or basic demographic information;
- The costs to collect and transmit data have not been factored into payment or financial considerations;
- Insights or results from study are not being shared back with Partners or affiliated hospital/institution.
- Data request is outside the original scope of work; or
- The request is for a significant amount of data.

For a MTA:

- Tissue sharing request intends to leverage tissue solely as part of a product development or commercial validation study;
- Tissue sharing request includes more than the following de-identified data fields:
    - Tissue type (e.g., blood)
    - Disease status (e.g., health, lung cancer)
    - Demographic information (e.g., gender, age group)
- Tissue samples will be used to obtain whole genome or exome data;
- Tissue samples are limited to patient specimens that may be important for future clinical and/or research use;
- The cost to collect and transmit samples have not been factored into payment or financial considerations;
- Insights or results from study will not be shared with Partners or affiliated hospital;
- Scope of use includes secondary use to leverage tissue or derived data as part of product development, validation study or other commercial activities; or
- Tissue request is outside the original scope of work.

If a data sharing request is referred to the PDTSC, the referring TAG or CTO staff and the PDTSC staff will work with the investigator to identify materials necessary for PDTSC review and approval.

Where to go/What to do

Genome-Wide Association Studies (GWAS) Data Sharing

Outgoing GWAS Data

In 2008, the NIH established a policy requiring sharing of GWAS data through the NIH GWAS repository for NIH funded applications and contracts submitted on or after January 25, 2008. A GWAS study is one in which 100,000 or more SNP markers are tested in individual DNA samples. The institution receiving the funds, through the PI, is responsible for submitting the data. Each submission must include a letter of certification signed by the Institutional Official. This letter certifies that the IRB has reviewed and verified the following:

- That the submission of the data is consistent with the informed consent signed by study participants from whom the data were initially obtained;
- Data-set de-identification is consistent with GWAS standards;
- Risks to individuals, their families and groups or populations associated with the data submitted have been considered; and
- Genotype and phenotype data were collected in a manner consistent with the Common Rule.

Therefore, the submitting PI must provide the following documents to the IRB:

- Description of what genotype/phenotype data are being submitted to the NIH;
- Copy of consent form(s) used at all sites to collect the initial data/samples; and
- Description of the method(s) used for coding data.

The NIH has developed an interactive overview of the GWAS submission process. PIs with GWAS awards should consult this document and work with the IRB and Partners Research Management (bwhsubs@partners.org; mghsubs@partners.org; mclsubcontracts@partners.org; SRHGC@partners.org)

Incoming GWAS Data

In order to access GWAS data held by the NIH, a PI must submit an application through the NIH National Center for Biotechnology Information Geneotypes and Phenotypes Database NCBI dbGaP Data Request System. The NIH has established stringent security requirements for institutions and investigators who receive GWAS data that must be agreed to by the appropriate hospital Signing Official through Partners Research Management. Submission of a GWAS application is limited to individuals with PI status. All data users should be listed on the GWAS application and, because these applications are institution specific, only data users from a single institution may be included. When submitting a GWAS application through dbGaP, PIs will be asked to select a Signing Official for

notification and approval of the application on behalf of the hospital. Information on whom to select is available via the hospital-specific mail boxes listed above. The Research Management Signing Official will refer the PI to Research Computing to review and fulfill the NIH data security requirements. In addition, a PI Memo and User Certification summarizing the terms of use will be issued.

Upon receipt of a signed User Certification from each data user and confirmation by Research IS Computing that the data security requirements have been met, the GWAS application will be submitted by Research Management. Shortly thereafter, the PI will be notified by NIH the application has been approved and the data will be made available. NIH requires submission of annual reports through dbGaP. Upon receipt of the GWAS data, the project's data management plan should be modified to reflect any requirements and the data managed accordingly.

NIH Genomic Data Sharing (GDS) Policy

The NIH GDS Policy applies to investigators who are conducting NIH-funded large scale (identifiable and de-identified) genomic research, and investigators who deposit genomic data or tissue into NIH repositories (required by some collaborators, publications, and some funders including NIH). NIH has strict standards for IRB review and informed consent for the human genomic data it will accept for inclusion in public data repositories regardless of whether your project has NIH funding. The NIH policy was effective 1/25/15 and applies to the following:

- NIH-funded research that generates **large-scale** genomic data (e.g. SNP arrays, genome sequencing, RNA sequencing, transcriptomic, metagenomics, epigenomic and gene expression data, GWAS studies) from more than 100 individuals. The policy also applies to subsequent research studies that use this type of data (secondary use).

For the most current NIH requirements and guidance, we recommend investigators review the NIH Genomic Data Sharing (GDS) website and NIH GDS FAQs.

For existing research using or generating genomic data, the IRB is required to review investigators' submissions to NIH data repositories. The primary focus of the review is on whether informed consent has been obtained from subjects in a manner consistent with NIH requirements for sharing genomic data and whether the data sharing plan is consistent with GDS policy. An Institutional Certification is required to deposit data or tissue into NIH repositories.

For all NEW grant applications that request NIH funding for genomic research, a genomic data sharing plan consistent with GDS policy must be included in the NIH application. If genomic data are being generated, the NIH GDS policy requires an Institutional Certification as part of the Just-in-Time submission, as well as a Certification at the time of data submission to a data repository.

NIH Data Sharing Plan Requirements

The NIH requires submission of a data sharing plan for all investigator-initiated applications and proposals with direct costs greater than $500,000 in any single year. Applicants should discuss the data sharing plan with their Program Officers at the time they request approval to submit an application over $500,000. When NIH makes the award, the data sharing plan automatically becomes an award term. Like any award term, failure to distribute data in accordance with the plan or any other deviation from the data sharing plan would be considered non-compliance by the NIH.

NIH instructions related to data sharing plans as they apply to applications and proposals responding to a specific Request for Application (RFA) or Request for Proposal (RFP) are always described in the solicitation. In some instances Program Announcements (PA) may request data sharing plans for applications that are less than $500,000 in direct costs in any single year. When submitting an application, PIs should provide all data sharing information requested in the PA.

The NIH recognizes that data sharing may be complicated or in some instances may be limited by institutional policy. The rights and privacy of individuals who participate in NIH research must be protected at all times. Data intended for broader use should be free of identifiers that would permit linkages to individual research participants and variables that could lead to disclosure (HIPAA identifiers). Partners investigators are required to follow the Partners data sharing policies and procedures identified and/or outlined in this document. Questions should be referred to the IRB, the hospital Privacy Officer, or hospital Research Compliance.

General questions on what to include in basic data sharing plans in NIH applications and proposals should be referred to the Partners Research Management Pre-Award Grant Administrator who supports your department.

Retention of Data Provided Under DUA

Regardless of source (e.g., industry, federal agency or non-profit institution) data retention is limited to the scope of the project. Any data retention, destruction or return requirements set forth in the DUA must be adhered to by the PI.

5. Data Security

Thoughout each stage of the Data Life Cycle, investigators and research staff are responsible for taking steps to secure Research Data from unintentional and intentional loss or theft. Every research record represents an investment of time, energy, talent, and money. As Research Data stewards, PIs, investigators, research staff, and the hospitals have an obligation to keep Partners Research Data safe

from loss, theft, or accidental destruction (water damage, fire, etc.) regardless of the data classification. The steps to secure Research Data depend not only on the sensitivity of the specific data and whether paper-based or electronic-based, but also on the Research Data's importance to the overall research operations of the group. What if staff members were unable to access the Research Data for a day, a week, or a month? What if the Research Data became entirely unusable? Could the research group still complete its research activities and fulfill grant or contract requirements?

Paper-Based Records

Paper-based records, including but not limited to bound laboratory notebooks, must always be stored in a secure location: a locked cabinet, container or vault in a secure room. For human subjects research, when determining where or how to store paper-based Research Information or records, PIs and their staff should review consent forms and protocols for storage commitments made to research subjects and regulatory requirements and make their storage arrangements accordingly. Laboratory notebooks that contain PHI must always be stored under lock and key. Access to PHI is limited to IRB approved study staff.

Records that include information that will be filed in support of a patent application and/or that include proprietary information must also be stored in locked areas with limited access controlled by the PI.

The PI is responsible for reviewing contract documents for sponsor-specific storage requirements, e.g., Federal Information Security Management Act (FISMA) requirements in federal contracts, and make their storage arrangement accordingly.

Original laboratory notebooks may not leave the research area, except for storage at an approved off-site vendor.

Storage of paper-based research data or records at the PI or a staff member's home is unacceptable and a violation of Partners policy.

Public Research Data on paper should also be protected against forgery and modification through secure storage, as should institutional data. Confidential Research Data may not be copied without the appropriate authorization from the PI or the sponsor, if sponsor approval is required under the award's terms and conditions. If copied, the Research Data or Research Information must be secured in transit: transported in a locked briefcase until arrival at the final destination or through certified transport (USPS or Federal Express.) The most secure and preferable means of transport is electronic. Confidential Research Data should be scanned and protected and transported in accordance with Partners policies. Questions should be referred to the hospital's Information Security Officer (ISO).

Electronic-Based Records

Electronic Research Information (records and Research Data) must be protected at rest and in transit. Proper authorization mechanisms (passwords) must always be used, in addition to encryption, to prevent unauthorized access to data or other records. Partners-approved software and Research IS Computing supported applications like REDCap and LabArchives contain some of the required protections within the programs themselves.

Security controls include:

- Password protection for all computers, tablets, mobile devices.
- Current, up-to-date operating system and anti-virus software on all electronic devices.
- Limiting access to laboratory systems, information and data to minimum necessary for employment or training.
- Disk encryption software on computer and mobile devices.
- Data redundancy through back-ups.
- Activity log-in requirements and audit-trails.
- Data storage in restricted access areas within the Partners' computing network.
- Using secure password protected networks (not public WiFi or unknown networks.)

Physical security measures include:

- Locking a computer when you walk away from it.
- Awareness of your surrounding area when using mobile devices in public places.
- Storing computers, laptops, and tablets in locked areas. Use device locks to secure laptops to a desk or work area during use.
- When traveling, never check computers, laptops, or tablets with luggage. You should carry these items with you.
- Never use portable storage media, such as flash drives and disks, for the long-term data storage. If you must use portable storage media, the device must be encrypted.
- Maintain an inventory of all computer and mobile electronic devices.

Additional Requirements for Confidential and Protected Health Information

Data involving human subjects research or PHI require greater protection than other data types. The Health Information Portability and Accountability Act ("HIPAA") protects personal health information from being disclosed without prior authorization from the patient or approval of a waiver of authorization from a Privacy Board. At Partners, the IRB serves as the Privacy Board. HIPAA encompasses Research Data that is created through clinical activities at a Covered Entity (i.e., the hospital) or involves the use of identifiable protected health information at a Covered Entity Using the least amount of identifiable information will not only reduce the researcher's regulatory burden, but is also required by Partners policy and HIPAA.

HIPAA coverage of Research Data can vary among institutions. Partners covers Research Data that are generated solely for research, as well as any clinical data that are used in research. Any PHI that enters a Partners hospital is covered by HIPAA as soon as it enters the Partners system.

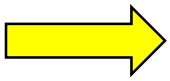
For more information, please consult these policies on PHI

- Partners Healthcare Inc. Definition of Protected Health Information
- Partners Healthcare, Inc. Minimum Necessary Policy
- Partners Healthcare, Inc. Accountability of Electronic Media Policy

Electronic Research Data are considered "secure" if they are rendered unusable, unreadable, or indecipherable. The only acceptable method for securing electronic data is encryption. Smartphones (iOS and Android), iPads and tablet, laptops, portable data storage media, and personal desktops used to conduct Partners business must be encrypted using a Partners approved product.

Other Security Concerns

Email Security



All communications regarding Partners Research Data must be sent through the Partners email system using Partners email domains and not through other accounts or email systems, e.g., Gmail or Yahoo mail.

As required by Partners policies, the confidentiality of all Research Data, whether proprietary or PHI, must be considered before any data are sent via email. Files or messages containing health information must be sent on a "need-to-know" basis. All official notifications to research staff from the Institution should be sent through the employee's partners.org email address or the hospital-specific email address, e.g., @mgh.harvard.edu. Employees may not use personal email accounts when transacting Partners business.

When sending PHI or other Confidential Information to collaborators and others outside the Partners firewall, investigators should use one of the secure file transfer solutions approved by Partners Research Computing. Tools like Send Secure Encrypted Email, Secure File Transfer Web Conferencing, Dropbox Business and Syncplicity are offered and supported by Partners IS.

MobileIron

MobileIron is software used by Partners to provide easy access to Partners resources from mobile devices. As of 10/31/17, all mobile devices accessing Partners email must be enrolled in MobileIron. Enrollment information for different systems (i.e., iOS and Android) is available at the following site: https://pulse.partners.org/resources_training/wikis/is/is_wiki_item/mobileiron_facts.

Password Security

Individual passwords to institutional (i.e., laboratory, hospital, or Partners) systems and/or devices must be kept confidential and must never be shared. Passwords are used to limit access and maintain accountability within systems; therefore, each password must be associated with a single individual. IS does offer the option of establishing a "service account" when a generic (usually group) password is required, for example, to operate a piece of common equipment. The password is managed automatically through a tool called CyberArk. PIs should contact the hospital Information Security Officer if interested in establishing a service account for their research group. IS will determine whether such an arrangement is possible.

Passwords must be changed in accordance with Partners policy and should be a unique alpha, numeric, and special character sequence. For more information on use of passwords, please consult the Password Management Policy.

6. Data Retention

Partners institutions and their investigators, research staff, and administrators share responsibility for the retention of Research Data. Research sponsors are the primary source of retention requirements through the grant or contract agreement that provides the funding. Federal, state and local governments are also a source of minimum retention requirements through individual agency policies or regulations or, in the case of federal awards, through the Uniform Guidance. Additional obligations may be imposed by journals as a condition of publication. On occasion Partners may require a retention period longer than the minimum for certain business operations or possible legal actions.

In accordance with Partners Policy, Research Data and Research Information should be kept no fewer than seven (7) years after the end of a research project or activity. In this context, a research project or activity should be considered ended after submission of (whichever is later)

- Final technical report to sponsor;
- Final financial close-out of a sponsored research award (i.e., submission of final financial report and close-out documents;
- Final publication of research results;
- Termination of activity on a research project regardless of whether results are published; and
- Any end date otherwise defined in the research/sponsorship/data use agreement (if any) governing the project.

If Research Data are/were the subject of a legal action, they may be held from destruction by notice from the Office of General Counsel. Standard hospital medical records, employment records, and business records should be kept in accordance with the appropriate Partners policy.

Please consult the Partners Guidelines on Retention of Research Data, Materials and Records, for all retention requirements.

7. Data Destruction

Confidential paper-based Research Data must be shredded before they are discarded. Locked metal boxes are located throughout the hospital for disposal of paper-based Research Information. Items in these boxes will be shredded by an outside vendor and then discarded. Research Information stored on portable storage media, such as a flash-drive or disk, may be disposed of in specially marked bins located throughout the hospital. Items in these boxes will be destroyed and recycled by an outside vendor in a HIPAA compliant manner. Contact Research Computing to remove Confidential Information from devices that may not be destroyed, such as computers.

8. Data Transfer When Investigators Leave Partners

When investigators leave the hospital or institution for other opportunities, they often want and may need to take Research Data with them. Because ownership of all Research Data rests with the Institution, original Research Data should generally remain at the Institution within the investigator's department. Departing investigators may make copies of their Research Data to bring with them to their new institution.

As we go to press, we are updating and revising transfer-out guidance documents which include detailed information on what investigators are required to do when leaving a Partners institution. In the meantime, investigators should rely on existing guidance. Before leaving, consult the Partners IRB for transfer of Human Subjects data and Partners Research Management for transfer of Research Data associated with a Federal award. Other questions should be directed to the hospital Research Compliance or Corporate Compliance office.

9. Data Integrity

Data integrity is a measure of a project's accuracy and reliability. Producing accurate and reliable Research Data is a goal of scientific experimentation. Data integrity protections should be built into every aspect of the research endeavor regardless of whether the project is basic, clinical or applied research.

- The Protocol
    - Create standardized procedures and protocols for actions that will be repeated over time. Periodically check to be sure these procedures are followed.
    - Include the appropriate controls in each experiment to demonstrate that each aspect of the experiment is working as expected. Controls should be repeated with each experiment.
    - To the extent possible, standardize materials using consistent vendors and catalog numbers.

- Laboratory Instruments and Machinery
    - Test the validity of laboratory instruments when they first enter then lab and periodically thereafter, to ensure that they are operating as expected.

- Data Collection and Recording
    - Create random spot checks in the data collection process to ensure data are being collected and reported as expected.
    - Where possible add procedures that will flag data entry errors, such as limiting the possible values that may be entered, or requiring double entry for large data sets.

- Specimens, Cell Lines, and Animal Colonies
    - Check periodically to be sure that cell lines and animal colonies still display the genotypic and phenotypic traits expected by the researcher.

10. Security Incidents: Lost or Stolen Laptops and other Data Losses

Whenever an electronic device is lost, stolen, or accessed inappropriately, the owner must contact the appropriate institutional Privacy Officer immediately upon discovering the electronic device is missing. Any delay in reporting could adversely impact the Institution's reporting requirements and could escalate the repercussions in the event of a security breach. Upon receiving a report of loss, theft, or inappropriate access, the Privacy Officer will assess the type of information that was stored on the device, the type of security measures that were enabled, and the risk of harm from an unauthorized disclosure.

The institution's Privacy Office and Partners Information Systems are the only offices authorized and able to determine the nature and scope of a potential unauthorized disclosure. This assessment may not be made by the individual owner of an electronic device; therefore, every incident of a lost or stolen electronic device must be reported to the Privacy Office. If the lost or stolen item is a smartphone or mobile electronic device, please contact the Partners Healthcare IS Helpdesk before

contacting your service provider. The Helpdesk can remotely erase data stored on these devices, but only before the service is terminated. Once the service provider terminates service the Helpdesk will not be able to protect any of the information stored on the device.

Loss or theft of paper-based Research Information such as patient surveys, laboratory notebooks or research binders that contain PHI must be reported immediately to the institutional Privacy Officer. If PHI associated with an IRB-approved clinical research protocol is lost or stolen, this information must also be conveyed to the IRB as soon as possible. Any loss of Research Data, regardless of whether PHI is included, should also be reported to the Partners Office of Research Compliance.

11. Where to go with questions

Brigham and Women's Hospital Research Compliance
Lisa Griffin, lgriffin11@bwh.harvard.edu

Massachusetts General Hospital Research Compliance
Mary Gervino, mgervino@partners.org

McLean Hospital Compliance
Jennifer Mahoney, jmahoney12@partners.org

Spaulding Rehabilitation Hospital Compliace
Monica Baggio Tormey, mbaggiotormey@partners.org

MGH Institute for Health Professions
Robert Hillman, hillman.robert@mgh.harvard.edu

Newton Wellesley Hospital
Maureen Dwyer, mkdwyer@partners.org

For general questions
Partners Research Compliance- phsrcr@partners.org

Acknowledgements

We would like to acknowledge the contributions of all who participated in the development of this guidance document.

Authors

Chris Clark, JD
Lisa Griffin, JD
Emily Sobiecki, JD
Fabio Martins
Mary Mitchell

Individuals asked to review drafts or contribute content

Dennis Brown, PhD
Chris Beares, JD
Alisa Busch, MD
Kim Durniak, PhD
Jose Florez, MD, PhD
Shelly Greenfield, MD, MPH
Libby Hohmann, MD
Jigar Kadakia
Adam Landman, MD
Maureen Lawton, JD
Andrea Messina
Debbie Mikels
Karen Klar Miller, MD
Megan Morash
Danielle Morin
Suzanne Morin
Allison Moriarty
Shawn Murphy, MD, PhD
Pearl O'Rourke, MD
Kerry Ressler, MD, PhD
Brent Richter
Paula Sciabarrasi, JD
Lynn Simpson
Heather Shea, JD
Stephanie Stone, JD
Beth Watters, JD
Scott Weiss, MD