USE OF DATA AGREEMENT
For Research and/or Healthcare Operations
By Johns Hopkins Workforce Members

THIS USE OF DATA AGREEMENT (the “Agreement”) is between the person signing below (“You”) as the Principal Investigator (if a research protocol) OR Project Leader (if a health care operations activity) OR as a Johns Hopkins workforce member conducting routine activities (Workforce Member), and The Johns Hopkins University or The Johns Hopkins Health System entity or entities providing You with the data (“Data Provider”). The Agreement takes effect on the date signed by You.

PURPOSE

Under state and federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 and its regulations ("HIPAA"), Data Provider must protect the privacy, confidentiality and security of certain information that it maintains (the “Records”).

Research and health care operations (including particularly quality improvement activities) have become increasingly important for Johns Hopkins University and Health System entities and departments. Routine operations also frequently are data driven. These activities often require large data sets from multiple clinical and operational sources. In aggregating and analyzing these data sets there are certain privacy and security risks. Data analysis therefore requires parameters around the collection, handling and disposition of critical data sets, including those containing Protected Health Information (PHI) or derived from PHI, Personally Identifiable Information (PII), de-identified data, or other sensitive data.

You are conducting one or more studies that have been approved by a Johns Hopkins Institutional Review Board (IRB) (the “Protocol”) OR are undertaking health care operations activities such as quality improvement reviews or routine operational activities (the “Operations Activity”) (the Protocol or Operations Activity being individually and collectively referred to hereafter as the “Project”). If required, each Project has or will have been reviewed by the appropriate review body designated by Johns Hopkins to oversee use of large clinical data downloads (such as the Clinical & Quality Data Sub-Council or Research Sub-Council of the Data Trust Council, or the Center for Clinical Data Analytics)(as applicable, the “Review Body”) and is consistent with the recommendations of the Review Body. If an Operations Activity, each Project also has or will have the approval of Data Provider.1 In connection with your Project You wish to access the Records or receive a subset of the Records (including de-identified data or a limited data set, all collectively referred to as the “Data”). Before granting You access to the Records or Data, Johns Hopkins requires You to agree to and abide by the terms and conditions described in this Agreement.

AGREEMENTS

YOU agree as follows:

1. Grant of Access. Your access to the Records is for a limited period of time and solely for purposes of the Project, and is subject to the terms of this Agreement.

2. Your Obligations.

---

1 Data Provider approval will be deemed to have been obtained for any workforce member whose job responsibilities entail being involved in “Operations Activities” on a routine basis for a significant amount of their daily tasks. Otherwise, in the absence of a recognized group of the Data Provider to grant approval, approval of the Data Trust Council or one of its sub-councils is required.

1/28/16
2.1 **Representation.** You represent that you are a workforce member of an entity within Johns Hopkins Medicine.²

2.2 **Compliance with this Agreement.** You, as the Principal Investigator, Project Leader or Workforce Member, are responsible for ensuring that Data are shared

(i) if your Project is a Protocol, only with members of your IRB-approved study team and, if outside parties are involved, only with those who have signed a “Confidentiality Agreement from a Third-Party in Johns Hopkins Research Protocol” or equivalent agreement;

(ii) if your Project is an Operations Activity, only with those Johns Hopkins workforce members necessary to perform the Project and, if outside parties are involved, only with those with whom a HIPAA Business Associate Agreement has been entered into;

and that each individual on the Project team (including any outside party) is aware of and abides by the terms and conditions of this Agreement. (“Outsiders” (subcontractors and the like) must sign an agreement to so abide with the terms and conditions of this Agreement.) You, as the Principal Investigator, Project Leader or Workforce Member, also are responsible to pass along this Agreement and these obligations to any successor Principal Investigator, Project Leader or Workforce Member on the Project.

2.3 **Permitted/Prohibited Access, Use and Disclosure.** You agree that You will access the Records, and obtain the Data, only for the purposes or the activities which have been authorized by Data Provider or the IRB, and/or Review Body, as applicable. Accessing, using or disclosing the Records or the Data for any other purpose is prohibited without the prior written consent of Data Provider, the IRB and/or the Review Body, as applicable.

2.4 **Minimal Access, Use and Disclosure.** You will make reasonable efforts to access only the minimum number or amount of Records necessary for your analysis, and to use and or disclose no more than the amount of identifiable information in each Record that is the minimum necessary to accomplish your purpose. You agree to maintain the confidentiality of all information contained in any Record that you access.

2.5 **Conditions of Access.** You agree:

a. Not to use or further disclose the Data or any information contained therein other than as permitted by this Agreement or required by applicable law.

b. To report promptly to the Johns Hopkins Privacy Officer any unauthorized access to Records or use or disclosure of the Data or any part of it not provided for by this Agreement of which You become aware.

c. Not to grant to others, or allow others to have, access to the Records or the Data (other than those identified in Section 2.2 above) without prior Data Provider approval. If Data Provider grants approval, and

(i) if your Project is a Protocol, You must (A) notify, and obtain the prior approval of, the IRB, and (B) if the others to whom access is to be granted are not employees or faculty of a Johns Hopkins University or Health System entity, provide Data Provider copies of signed “Confidentiality Agreement(s) from a Third-Party in a Johns Hopkins Research Protocol” or equivalent agreement; or

---
² Those whose primary appointment is in, or who are employed by, The Johns Hopkins University Bloomberg School of Public Health are not workforce members of Johns Hopkins Medicine.
(ii) if your Project is an Operations Activity and your Project team includes members who are not employees or faculty of the Johns Hopkins University School of Medicine or School of Nursing, or a Johns Hopkins Health System entity, provide Data Provider signed copies of a HIPAA Business Associate Agreement or HIPAA Data Use Agreement approved by the Johns Hopkins Privacy Office, as appropriate.

d. Not to maintain an independent copy of the Data unless specifically authorized by the terms of the approved Protocol or Operations Activity and then only subject to the terms of this Agreement.

2.6 Security of Electronic Information. You specifically agree to use appropriate safeguards to prevent use or disclosure of the Data or any information contained therein other than as provided for by this Agreement. Those safeguards, at a minimum, shall include:

a. that access is managed through authorization and authentication is managed through unique accounts and de-provisioned as appropriate;

b. that a current list of individuals authorized to access the data set is maintained and individuals no longer authorized to access the data set are removed promptly;

c. that Data are not transmitted outside of Hopkins or stored on portable media or devices (e.g., laptops) unless encrypted;

d. that Data are stored only on a managed Hopkins server that is configured and monitored according to Hopkins standards; and

e. that all devices used to access the Data be 1) managed by IT at Johns Hopkins, 2) use the Virtual Desktop Interface for data access, 3) use remote desktop for data access, or 4) have up-to-date patching (e.g., OS Flash Java) and endpoint/anti-virus protection (e.g., MS Endpoint protection).

3. Termination for Breach. Data Provider shall have the right, in its discretion (i) to notify You that You are in breach of this Agreement, and to give You a reasonable time period (not to exceed thirty (30) days) to cure such breach, or (ii) to terminate this Agreement and thereby end your right of access and/or use of the Data. Any termination for breach also may result in further investigations to determine whether there have been violations of other standards, policies or protocols (such as HIPAA or IRB or Human Resources policies).

4. Expiration of Agreement. This Agreement shall expire on the later to occur of (i) the end of the Protocol or the end of the IRB approval of the Protocol, (ii) the completion of the Operations Activity, either as applicable, and (iii) one year from the date of the signature below.

5. Obligations Following Termination. Upon expiration or termination of this Agreement, You shall no longer be entitled to have access to the Data. At that time either:

a. You must return and/or destroy all Data received directly or indirectly from or on behalf of the Johns Hopkins Data Provider and You (including any member of your study team) must retain no copies of such Data

or

b. If it is not feasible for You to return or destroy the Data, You will use such Data only as permitted by this Agreement and You will continue to apply the protections of the this Agreement to such Data;
and

c. You must cause any “outside party,” agent or subcontractor to whom you provided Data to return or destroy all of such Data and no “outside party,” agent or subcontractor, to the best of Your knowledge, shall retain any such Data.

6. **Assignment.** You may not assign your rights or obligations under this Agreement to any other person or entity without the prior approval of Data Provider.

**IN WITNESS WHEREOF,** You have signed this Agreement to be effective on the date set forth below.

Signature: ____________________________

Printed Name: _________________________

Title: ________________________________

Date: ________________________________