Data Security Profile (Version 1/30/19)

PI/Requester Name:

Study name (if applicable):

IRB # (if applicable):

This document details security controls you will put in place for Data you receive or create to complete research, quality, or operational projects. The profile applies to Data containing Protected Health Information (PHI) or derived from PHI, Personally Identifiable Information (PII), de-identified data, or other sensitive data. We encourage those storing Data to use consistent best practice security measures for all projects. Complete this document describing your security practices. Once the document is reviewed and approved by the appropriate parties, you may use the profile for data requests for a one year period.

This document is designed to cover areas of particular concern but is in no way exhaustive. You should also review the JH policies, standards, and guidance on HIPAA compliant use of Data and consider the specific risks related to the electronic storage of Data before completing the profile.

The document should be updated at any time you make substantial changes to Data or its configuration, as well as at the time of submission of your continuing review application. For comments and questions about use of electronic systems that contain PHI, please contact itpolicy@jhu.edu.

Questions regarding completion of this document should be directed to ITRisk@jhu.edu.

Responses to this form must be typed and saved as a word document as it may be required for data request processes.

1 Describe where the data will be stored and analyzed.

Pick all that apply.

☐ The project will use the ICTR SAFE Virtual Desktop and SAFE secure file share to store and analyze data.
For information on how to obtain a SAFE virtual desktop for data storage and analysis, visit https://ictr.johnshopkins.edu/safe-desktop or email bonnie.woods@jhu.edu.

☐ The project will store data on a departmental file server with appropriate restrictions in place to limit file access and analyze data on an on-premises managed desktop or encrypted laptop.
For information on department file servers, managed desktops, and laptop encryption, contact your LAN Administrator or your division or department IT Help Desk.

☐ The project will use JH-managed OneDrive to store data and share data with internal project members and 5 or fewer external investigators. **By checking this box, I attest that I have reviewed and will apply the instructions on configuring OneDrive (http://www.it.johnshopkins.edu/services/collaboration_tools/OneDrive/Configuring%20OneDrive%20for%20Secure%20Sharing.pdf) for secure sharing.**

☐ The project will use JHBox to share data with internal project members and 5 or fewer external investigators. Internal project members will analyze data on an on-premises managed desktop or JH-managed and encrypted laptop.
By checking this box, I attest that I have reviewed and will apply the instructions on configuring JHBox for secure sharing. (www.it.jhu.edu/jhbox/securesharing/tips.pdf).

☐ The project will use JHU REDCap (see http://redcap.jhu.edu/).

☐ The project team sends or inputs PHI, including a limited data set, into a system at a partner institution, e.g. a data coordinating center, and the partner institution has shared a HIPAA-compliant security plan with the investigator that details encryption, patching, and multi factor authentication.

☐ Other
Complete the Data Security Checklist (: https://johnshopkins.service-now.com/serviceportal/?id=evg_sc_cat_item&sys_id=d4f840900f776200976b9bd692050e65#). If you have an IRB application, upload it to your IRB application, section 20, question 2. It will be reviewed by the appropriate security and privacy experts.

2 Describe Access Provisioning and De-provisioning

Access must be managed through authorization, and authentication must be managed through unique accounts and de-provisioned in a timely manner. Only those individuals with a business need to access Data are authorized to have access. Principal investigators/project leaders must address whether a user has a need-to-know and whether the minimum necessary Data is made available for access. See the following for more information: http://intranet.insidehopkinsmedicine.org/privacy_office/privacy_topics/ways_to_communicate.html

1	Do you have a documented process for adding and quickly removing individuals from the authorized access list (hence terminating access to Data)? Describe your process for managing access to the Data.	
2	Who authorizes access?	
3	Do authorized individuals use JHED for login to access data?	
4	Do you communicate to Data users that they are prohibited from using email messaging for transfer and must use Johns Hopkins file sharing services instead?	

3 Data Minimization

All projects should minimize the data used to the greatest extent possible (See data minimization guidelines: http://intranet.insidehopkinsmedicine.org/data_trust/_docs/data_minimization_guidelines.pdf).

For research studies, it is a best practice to maintain separate raw-data and analytic files, with a link table connecting PHI identifiers (for example, medical record number) in the raw data file(s) to an anonymized study ID in the analytic file(s). To the extent possible, access to raw data files containing PHI should be limited to the study data coordinator or database administrator. As a best practice, individual research assistants/abstractors will not have global data access, and will not be able to copy the research database.

Describe any steps you take to minimize the data used for analysis.

4 Other Risk Factors

There may be unique characteristics of the project for which the data are used that would create additional privacy and security risks (e.g. adoption of untested technologies, possible expansion of scope, extraordinary regulatory requirements [Europe, FISMA]). Please discuss these below if any and your approaches to mitigate risk.

If end users will have global equivalent access to the underlying Database, that should be noted.

	Risk Factor	**Mitigation Control**

If you require assistance in developing your e-PHI application to be HIPAA compliant, please contact itpolicy@jhu.edu

5 Attestation

All individuals on the Project team are aware of and abide by the terms and conditions of the Johns Hopkins Use of Data Agreement, which includes the following requirements:

a. that access is managed through individual JHED accounts;

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 is not transmitted outside of Hopkins unless encrypted;

d. that Data is not carried on portable media or devices (e.g., laptops) unless encrypted;

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

f. that all devices used to access the data 1) use the Virtual Desktop Interface for data access, or2) have up-to-date patching (e.g., OS Flash Java) and endpoint/anti-virus protection (e.g., MS Endpoint protection).

By submitting this document, I attest that the responses are complete and accurate to the best of my knowledge and that collaborators are following requirements set forth in the Johns Hopkins Use of Data Agreement.

Name:

Date submitted:

Reviewed by:

Review Date:

Decision: