Section 12: Privacy and Confidentiality

In this section, you will be prompted to answer the following questions:

***Explain how you will ensure that the subject's privacy will be protected**

Consider privacy interests regarding time and place where subjects provide information, the nature of the information they provide, and the type of experience they will be asked to participate in during the research.

***Describe how research data will be stored and secured to ensure confidentiality**

How will the research records and data be protected against inappropriate use or disclosure, or malicious or accidental loss or destruction? Records and data include, for example, informed consent documents, case report forms or study flow sheets, survey instruments, database or spreadsheets, screening logs or telephone eligibility sheets, web based information gathering tools, audio/video/photo recordings of subjects, labeled specimens, data about subjects, and subject identifiers such as social security number.

Section 12.1: Research Data Security Plan

In this section, you should describe the types of information you will be storing and where it will be stored. It will be reviewed to ensure proper data security and management.

02.1 Storage of Paper or Non-digital Media

Indicate if paper or non-digital media, even if the storage is temporary, contain:	Please contact the School of Medicine Compliance Office if you have questions about de-identification of data.
* Social Security Numbers (SSN's) : Yes	
* Protected Health Information (PHI): Yes	
* Other sensitive information: Yes	

***Specify the location where paper or non-digital media will be stored**

***Specify who has access to the paper or non-digital media**

Indicated all people who have access, such as PI, Clinical Research Coordinator, Nurse, Research Assistant, other non-Key Personnel (e.g. finance).

***Specify how the paper or non-digital media are secured**

Examples:
-Documents including, but not limited to, enrollment log/case report forms (CRF's) containing SSN's are locked in PI's office, with key in custody of CRC
-Documents including, but not limited to, medical record numbers, are locked in PI's office with key in custody of Research Nurse

-Documents Including, but not limited to, study records are locked in PI's office, with key in custody of Research Nurse and CRC.

02.2 Storage of Electronic Information

Indicate if electronic research data, even if the storage is temporary, contain:

* Social Security Numbers (SSN's):	No
* Protected Health Information (PHI):	Yes
* HIV or mental health records:	No
* Other sensitive information:	Yes

Temporary store of electronic SSNs (permanently redacted at earliest possible time) may be permitted for participant payment purposes, but all other electronic SSN storage requires institutional approval through Duke Medicine ISO. All storage, temporary or permanent, must be listed within RDSP.

Indicate who is managing the infrastructure where electronic research data is stored:

* **Duke Medicine** Department Supported IT Service:	No
* **Duke Medicine** Lab Supported IT Service:	No
* **Duke Medicine** Managed IT Service:	No
* **Duke University** Office of Information Technology (OIT) Managed Service:	Yes
* **Duke University** Campus Department Supported IT Service:	No
* Durham Veteran Affairs:	No
* Other entity outside of Duke:	No

Duke Department Supported IT Service
a formal School of Medicine IT support group supports the servers and workstations on which research data resides.

Duke Lab Supported IT Service
a lab or other unit whose IT support is handled by a research associate or person with other similar duties, and has no formal departmental or managed support.

Duke Medicine Managed IT Service
within the IGSP, Cancer Center, and DTMI/DCRI. Note: these are examples only and have not been formally designated. Selection of a Duke Medicine Managed IT Service means that research data is maintained by one of Duke Medicine's Managed IT Service providers.

Duke University OIT Managed Service within a University OIT-managed service. This means that the research data is maintained and supported by an OIT service like the Protected Network.

Duke University Campus Department Supported IT Service within a campus school, institute, or department. Note: these are examples only. Selection of a campus department supported IT service means that research data is maintained by the researcher or IT staff within that organization.

Other Entities Outside of Duke This includes non-Duke Medicine entities, and outside sponsors, e.g. the study sponsor provides a web-based system into which research data is entered.

*If you are unaware of who is managing the infrastructure where research data is stored, please contact your SBR Administrator.

03. Duke Electronic Storage Details

* **Data is stored within a folder on one or more Duke file servers:** Yes

If yes: Specify the server name, server location, and the name of the folder that has been established by the IT Support Staff (e.g. server dhtsdata1 d:\documents…)

Data is being stored on a file server if the folder is "mapped" to the user's computer, such as a personal or department drive. Typically this data can be accessed from multiple computers and the computer is not physically located near the user.

* **Data is stored on one or more Duke desktop computers:** No

If yes: Specify the computer's physical location:

Data is being stored on a local desktop computer if the data is on a disk within the computer itself. The data is generally only accessible from this computer and the computer is physically located near the user (in the lab or office).

* **Data is stored on one or more mobile devices:** No

Mobile Devices include, but are not limited to: external hard drives, laptops, tablet PCs, flash drives, smart phones, PDAs.

***Mobile Storage Device:** any device which is designed for portability and is capable of storing data.

04. Software Environment & Survey Tools

* **Describe the software environment being used for research data collection and storage.**

Be as descriptive as possible. Include software names and version numbers. Include people responsible for managing the software / database / website, with their contact information.

Software environment examples:
* Microsoft Excel 2013
* Microsoft Access 2007
* Oracle, SQL Server 2008
* Apple, Linux, Unix
* Web interface for data entry or storage (list website)
* Sponsor/Web Portal (list website)
* Interactive Voice Response (VRS)
* Survey Tools such as REDCap Survey, Qualtrics, etc.
* Social Media (list website)
* Mobile applications (list name and details)