REDCap User Management Policy

<u>PURPOSE:</u>

To provide user management guidance and instructions for HPSH REDCap support staff.

<u>DEFINITION OF TERMS:</u>

REDCap	A web-based software program created by Vanderbilt University and supported by the REDCap Consortium to facilitate research and data collection. Partners HealthCare Research Computing ERIS in collaboration with the Harvard Catalyst	The Harvard Clinical and Translational Science Center offers the support and use of the service to HSPH personnel.
Super User	HSPH personnel responsible for user education and management of projects (ex: moving to production, approving changes when in production).
Project	Database or survey implemented in EDC Application. A set of data entry forms, schedules and other REDCap instruments pertaining to a specific study or research project.
Project Owner	A person responsible for the conduct of studies (ex: academic, operational) data collection, including assignment of the roles and authorizations to use specific forms and functions of the REDCap project to the members of the project team.
Principal Investigator	A person responsible for the conduct of the clinical research study, including assignment of the roles and authorizations to use specific forms and functions of the REDCap clinical research database to the members of the research team. Principal Investigator may also be the Project Owner.

<u>POLICY STATEMENT:</u>

This procedure applies to all user maintenance operations that are performed by HSPH REDCap Super Users.

<u>PROCEDURES:</u>

A. Creating **New User Accounts for Users with HSPH (LDAP) Accounts**

1. REDCap is directly synced to Harvard Active Directory. Harvard Accounts will be used to access the application.

2. Use of White List in REDCap:

   LDAP authenticated users will <u>not</u> be able to access REDCap until they have been added to the Whitelist by a Super User Admin.

   Anyone not on the Whitelist that authenticates via LDAP will be given a message saying that they cannot access REDCap until an administrator adds them to the Whitelist.

B. New User Accounts for Users without HSPH (LDAP) Accounts

1. External access will only be granted to researchers on HSPH IRB approved research studies. HSPH faculty requesting access must be a PI or Co-PI on the approved protocol. Student PI's must have mentor sign off prior to requesting access to REDCap.

2. External users must be granted IRB approval prior to being granted access to the system. Submit a modification request to add any additional users to an existing REDCap Project.

3. Non-HSPH usernames are created by the REDCap Super Use with the following schema: first letter of the first name, up to 5 letters of the last name, and where necessary a number incremented in case of duplicates (ex: John Doe = jdoe3).

C. User Rights

1. Users are assigned minimum necessary rights and access to protected health information (PHI) based on job requirements*.*

2. Project specific user rights will not be assigned by REDCap Super User. The Project Investigator / Owner is responsible for assigning, restricting and maintaining the roles and authorizations for project members to use specific features and functions REDCap via the application's User Rights module.

3. In addition to the above and specific to projects collecting sensitive data or PHI (i.e. Level 3 data), it is the responsibility of the Project Owner to:

   - Assign only Full Data Export rights for projects with PHI to those individuals trained to protect PHI (ex: only download to encrypted mobile devices or)

   - Collect only minimally-necessary set of PHI (protected health information), in addition to those required by study design or operational requirements, to positively identify study subject during data entry phase

   - Manage access to the project to state and federal regulations protecting patient privacy and confidentiality (ensure that each user is granted the minimum amount of access needed to perform his/her duties).

D. Password and User Account Maintenance

If a HSPH user forgets their username and/or password, they must reset it at:
https://password.sph.harvard.edu/IDM/jsps/login/Login.jsf

If a non-HSPH LDAP user forgets their username and/or password, user will:
- Answer security questions to obtain account details via the application.
- Contact an REDCap Super User. Prior to sending account details, the Super User will re-verify the user's identity by confirming the email address and username.

E. Terminating User Accounts

1. Super Users can promptly remove or disable user access for persons and entities that no longer need access to REDCap.

2. Accounts are terminated if:
- Requested by a HSPH employee
- Notified by any personnel of employment termination
- External accounts are inactive for 90 days.
- Email addresses are no longer active

F. Re-activating Terminated / Suspended Accounts

After termination or suspension of external user account, accounts can be re-activated if a HSPH employee confirms request.

G. User Account Audits

REDCap Super Users reserve the right to:

- Audit user accounts at anytime to determine if accounts are still active or need termination.

- Notify and report to the HSPH IRB and/or Privacy Officer on the activity and unauthorized use of REDCap for any research projects and/or the unauthorized collection of sensitive data and/or PHI (Level 3 or above).

<u>OTHER</u> <u>APPLICABLE</u> <u>HSPH</u> <u>POLICIES:</u>
HSPH REDCap Appropriate Use Policy