ROSWELL PARK COMPREHENSIVE CANCER CENTER	**Roswell Park Comprehensive Cancer Center** Policy and Procedure	**Date Issued:**	**Number:**
Title: REDCap Projects		**Revision:**	**Effective Date:**
Prepared by: Information Technology		**Approved by:** Michael Sexton, General Counsel	**Page:** 1 of 2

A. GENERAL STATEMENT OF POLICY

This policy establishes the framework for protecting Protected Health Information (PHI) within the REDCap (Research Electronic Data Capture) application by enforcing rigorous access controls and restrictions on all users. These measures ensure compliance with applicable privacy regulations, including HIPAA (Health Insurance Portability and Accountability Act), and to safeguard the confidentiality, integrity, and availability of PHI.

B. SCOPE

This policy applies to all users of the REDCap application.

C. ADMINISTRATION

This policy is to be administered by Information Technology, and the Research Advisory Team

D. POLICY / PROCEDURE

Roles and Responsibilities

This section outlines the roles and responsibilities that all REDCap users must comply with.

All REDCap Users

- Users must submit all requests through ServiceNow, including the following items, by utilizing the links available on the REDCap homepage:
  - New user access
  - New project
  - Project modification
  - Notify of Internal Review Board (IRB) protocol Status or Member List changes
  - Other assistance
- Users must provide accurate and detailed project information, particularly when requesting a new project. This includes, but is not limited to, the

Principal Investigator's name, a study description, the Protocol ID, and whether PHI is involved.
- Users are permitted to add records to the project only after IRB approval has been obtained.
- Users are responsible for developing, tracking, and maintaining their own unique de-identified identifiers. The use of "PT-ID" is prohibited, as it is not a valid de-identifier within the REDCap application.

Security Administrators
- Upon receiving a new project request, the REDCap Security Administrator must verify that the requester has provided all required project details.
- The Security Administrator is responsible for confirming the accuracy and completeness of the required information before approving the request.
- Record creation rights will only be granted once confirmation of IRB approval is obtained.
- When a request for new user access to a project is submitted, the Security Administrator must confirm that the individual is recognized as a Study Team Member, as defined by the IRB.
- Upon receipt of Protocol changes, the Security Administrator is responsible for implementing the necessary modifications to the project.
- Security Administrators are responsible for conducting an annual audit to ensure compliance with institutional policies, including the requirements outlined in this policy.
- Responsible for collaborating with BRISR whenever a review, consultation, or interpretation of a protocol is required in the context of REDCap projects and users.

Biomedical Research Informatics Shared Resource (BRISR)
- Responsible for collaborating with Security Administrators whenever a review, consultation, or interpretation of a protocol is required in the context of REDCap projects and users.

E. DISTRIBUTION

This Policy and Procedure will be distributed to all Roswell Park Managers via the Roswell Park internal web page and to holders of backup hard copies of the manual. Managers are responsible for communicating policy content to pertinent staff. In addition, they are currently available at the policy and procedure page on I2. The policy will be available on the REDCap homepage.