

SAN JUAN BAUTISTA SCHOOL OF MEDICINE
Research Center

**REDCap GOVERNANCE, COMPLIANCE, AND
RESEARCH USE POLICY**

Document Control

Policy Number	RC-REDCap-001
Version	1
Effective Date	September 30, 2026
Last Revised	None
Policy Owner	SJBSM Research Center, in conjunction with the SJBSM Institutional Review Board (IRB); final approval authority rests with the Institutional Research Committee
External Guidance Referenced	Vanderbilt University Medical Center REDCap and eConsent Governance Guidance (as in effect on the Effective Date above; see REDCap Administrators for the current version/date on file)
Drafting Disclosure	This policy was drafted and iteratively revised with the assistance of Claude, an AI assistant made by Anthropic, under the direction, review, and editorial control of SJBSM Research Center and IRB staff. Regulatory citations and factual claims were checked against primary sources during drafting; content, judgment calls, and final approval remain the responsibility of SJBSM.
Research Center Director / Co-Director	Dr. Estela Estapé — e_estape@sanjuanbautista.edu Dr. Yaritza Inostroza — yinostroza@sanjuanbautista.edu
REDCap Administrators	Francisco Velázquez Cruz, IT Director — fvelazquez@sanjuanbautista.edu Dr. Linda Pérez, Research Center Assistant Director — linda.perez@sanjuanbautista.edu
IRB Director	Dr. Manuel Pérez Pabón — mparez@sanjuanbautista.edu

Prepared in alignment with the Office for Human Research Protections (OHRP), 45 CFR 46 (the Common Rule), and REDCap governance practices adopted by Vanderbilt University Medical Center and other academic research institutions.

Table of Contents

1. Purpose	3
2. Authority and Regulatory Basis	3
3. Scope	3
4. Definitions	4
5. Roles and Responsibilities	4
6. Development Mode vs. Production Mode	5
7. IRB Submission Requirements.....	6
8. Electronic Informed Consent (eConsent)	6
9. QR Codes, Survey Links, and Recruitment Materials	7
10. Data Security and Access Control	7
11. Research Data Management and Record Retention.....	9
12. Guidance for Describing REDCap Use in an IRB Proposal	10
13. Secondary Use of Data.....	14
14. Audits and Monitoring	14
15. Noncompliance and Reportable Events	14
16. Training Requirements	15
17. REDCap Citation Requirement	15
18. Policy Review	16
19. Regulatory and Institutional References	16

1. Purpose

This policy establishes San Juan Bautista School of Medicine (SJBSM) Research Center requirements for using REDCap (Research Electronic Data Capture) for research activities conducted under SJBSM's auspices. It defines institutional requirements for human subjects' protections, data governance, data security, record retention, and regulatory compliance, and aligns SJBSM practice with the Office for Human Research Protections (OHRP), the Common Rule (45 CFR 46), and REDCap governance frameworks used at Vanderbilt University Medical Center — REDCap's founding and coordinating institution — and other academic research institutions.

2. Authority and Regulatory Basis

This policy is issued under the authority of the SJBSM Research Center and the SJBSM Institutional Review Board (IRB); final approval authority for this policy rests with the SJBSM Institutional Research Committee. This policy is based upon:

- 45 CFR 46 (the Common Rule) — Protection of Human Subjects
- OHRP guidance documents, including Investigator Responsibilities FAQs, Revised Common Rule FAQs, and IRB record-keeping guidance
- Applicable FDA regulations, including 21 CFR Parts 11, 50, 56, 312, and/or 812, as applicable to the specific investigation (e.g., Part 312 for drug investigations, Part 812 for device investigations, Part 11 for electronic records/signatures)
- HIPAA Privacy and Security Rules, where research involves protected health information (PHI)
- REDCap Consortium governance and end-user agreement terms administered through Vanderbilt University Medical Center
- SJBSM institutional IRB policies and procedures

3. Scope

This policy applies to all faculty, staff, students, residents, fellows, investigators, research coordinators, collaborators, and any other individual who accesses or uses the SJBSM REDCap instance for research activities. It governs human subjects research, student projects, faculty research, clinical research, survey research, electronic consent, recruitment activities, and research databases, regardless of funding source or sponsor. It also applies to activities for which the IRB has determined that the activity does not constitute human-subjects research or is exempt, to the extent such activities use SJBSM REDCap resources.

4. Definitions

- **Development Mode** — A REDCap project status used for database design, instrument building, testing, mock QR code creation, and IRB preparatory materials. No real participant data, consent, or recruitment may occur in this mode.
- **Production Mode** — A REDCap project status authorized only after documentation of the applicable IRB approval or determination has been obtained; the only status in which real participant data may be collected.
- **Principal Investigator (PI)** — The individual with primary responsibility for the design, conduct, regulatory compliance, and data integrity of a research study using REDCap. The PI must be an SJBSM faculty member.
- **REDCap Administrators** — The SJBSM Research Center staff member(s) responsible for technical administration of the REDCap platform, including account provisioning, project setup support, and system maintenance.
- **Identifiable Data** — Data through which a participant's identity is or could reasonably be ascertained by the investigator, directly or through linked identifiers.
- **Audit Trail** — REDCap's automated, system-generated log of user activity, record changes, and data access within a project.

5. Roles and Responsibilities

Principal Investigator	Obtains and maintains all required IRB approvals or determinations; ensures REDCap project content (instruments, consent forms, recruitment materials) matches IRB-approved versions; protects participant confidentiality; limits and reviews user access on a least-privilege basis; retains study records for the required period; and promptly reports noncompliance to the IRB.
Institutional Review Board (IRB)	Reviews and approves protocols, recruitment materials, consent forms (including eConsent workflows), and participant-facing materials; reviews amendments; and provides ongoing human-subject protections oversight, including continuing review when required by 45 CFR 46, other applicable regulations, or the IRB's determination.
REDCap Administrators	Provides account creation and project-setup assistance, and performs system administration, security configuration, and maintenance of the REDCap platform. The REDCap Administrators may provide technical records, audit logs, user-rights information, and system assistance in support of an authorized compliance review, but do not independently make IRB or regulatory compliance determinations, do not monitor investigator compliance with approved protocols on an ongoing basis, and do not assume responsibility for unauthorized investigator activity, unless specifically designated to do so under institutional policy.

Research Center	Maintains institutional REDCap governance, hosts training resources, coordinates audits in conjunction with the IRB, and maintains this policy.
All REDCap Users	Use REDCap only for approved, authorized research activities; complete required training; safeguard login credentials; and report suspected data security incidents immediately.

6. Development Mode vs. Production Mode

Development Mode may be used for database design, testing, instrument creation, mock QR code generation, and preparation of IRB submission materials. No participant recruitment, consent process, or collection of real participant data may occur in Development Mode.

Production Mode may be authorized after documentation of the applicable IRB approval, including IRB approval for nonexempt human-subjects research, or an IRB determination that the activity does not constitute human-subjects research or is exempt, as applicable, and after functional/user-acceptance testing of the project is complete. Production Mode is the only status in which real participant data may be collected, and the REDCap Administrators may verify documented approval or determination status prior to production release upon request from the IRB.

Development Mode and Production Mode are REDCap system states, not IRB approval stages, and using them does not imply a two-tiered IRB approval process. SJBSM's IRB review results in one of the following determinations: full approval; a deferral requesting revisions or additional information, followed by re-review; or disapproval of the research. For exempt or non-human-subjects activities, the IRB issues the applicable determination in place of full approval. SJBSM's IRB does not use provisional, conditional, or interim approval as an institutional approval category. Development Mode carries no IRB approval status of its own and permits no participant contact of any kind. A deferral means the study has not been approved, and the REDCap project must remain in Development Mode — with no recruitment, consent process, or data collection — until the IRB issues full approval or an applicable determination upon re-review. A disapproval means the study may not proceed in REDCap in any form absent a new submission and a new approval determination.

For multi-site or cooperative research subject to a single-IRB (sIRB) requirement under 45 CFR 46.114(b) or an applicable federal sponsor's policy, "the applicable IRB approval" required before Production Mode may mean approval by the external IRB of record under an SJBSM-executed reliance agreement, rather than approval by the SJBSM IRB directly; the reliance agreement itself, not this policy, establishes which institution's determination governs. This policy's REDCap-specific requirements (Sections 7 through 12) still apply regardless of which IRB holds the approval.

7. IRB Submission Requirements

Investigators may submit the following as part of IRB review of a REDCap project:

- Study protocols and data management plans
- Consent forms and eConsent workflows
- Survey questions and data collection instruments (PDF exports or screenshots)
- Data dictionaries
- Mock or non-functional QR codes
- Recruitment materials and participant-facing text
- Prior to activation in Production Mode, when requested by the IRB: a final REDCap instrument export or PDF showing the finalized question wording, response options, and branching logic; and screenshots or configuration documentation confirming relevant survey and privacy settings (e.g., anonymous survey enabled, IP address and geolocation collection disabled), as described in Section 12

Active survey links or fully operational QR codes should be provided to the IRB only when specifically requested for review purposes; a live, functioning link is not required for standard submission.

8. Electronic Informed Consent (eConsent)

IRB approval is required before any REDCap electronic consent (eConsent) process is implemented or used with participants. Investigators are responsible for ensuring that the REDCap eConsent instrument matches the currently IRB-approved consent form, including all subsequent amendments, at all times. Any discrepancy between the REDCap eConsent instrument and the approved consent document must be corrected before further use and reported to the IRB.

REDCap eConsent must also satisfy applicable requirements of 45 CFR 46.116 and 46.117, including presentation of information in language understandable to the participant or legally authorized representative, adequate opportunity to consider participation and ask questions, appropriate documentation of consent, and provision of a copy of the consent information or document to the participant when required. For FDA-regulated investigations, the eConsent process must separately satisfy applicable FDA electronic-record and electronic-signature requirements, including those under 21 CFR Parts 11, 50, and 56, as identified in joint OHRP/FDA eConsent guidance. These requirements are consistent with relevant Vanderbilt University Medical Center REDCap/eConsent guidance and applicable SJBSM REDCap governance requirements.

When the REDCap eConsent framework is activated for a project, REDCap automatically records the participant's IP address as part of the electronic consent completion record, unless this collection has been disabled at the system level by the REDCap Administrators.

Investigators using eConsent must disclose this IP address collection in the consent document and account for it in the project's IRB submission. This is the only place in this policy that states this requirement; Section 10 (CAPTCHA/bot protection) and Section 12 (submission guidance) refer back to it rather than repeating it.

9. QR Codes, Survey Links, and Recruitment Materials

Participant-facing QR codes, survey URLs, and public survey links require IRB review and approval before distribution or use. Recruitment materials generated or distributed through REDCap (including SMS, email invitations, and public survey pages) must match the IRB-approved versions on file, except for changes necessary to eliminate an apparent immediate hazard to participants, which may be made prior to IRB approval and must be reported to the IRB promptly thereafter.

Other modifications to participant-facing recruitment content made without prior IRB approval constitute deviations from the approved research and must be reported to the IRB in accordance with SJBSM IRB reporting requirements.

10. Data Security and Access Control

Research data in REDCap must be protected using the following minimum safeguards:

- Least-privilege access — user rights are limited to the minimum necessary for a user's role on the study team
- Role-based permissions configured and periodically reviewed by the PI, who must reconfirm at least annually, or upon any change in study team membership, that the active user list for each project remains accurate and limited to current, authorized personnel
- Strong, unique account passwords; multi-factor authentication is required for any project that stores direct participant identifiers, and is otherwise made available and encouraged for all accounts
- Prompt removal of access for personnel who leave the study team or institution
- Use of REDCap's built-in de-identification, data access group, and field-level security features where appropriate to the study design
- Compliance with all applicable SJBSM institutional IT security and HIPAA security requirements

Institution-wide multi-factor authentication for REDCap has not yet been activated. The Research Center and IT Department are consulting to determine whether and when activation is

feasible. Until MFA is activated, projects storing direct participant identifiers must implement compensating controls approved by the REDCap Administrators (for example, restricted network access, shortened session timeouts, or heightened account-activity monitoring), and MFA will become a mandatory, enforced control for all such projects once institution-wide activation is complete.

Investigators are responsible for safeguarding data confidentiality and limiting access to identifiable data to authorized study personnel only. Suspected unauthorized access, disclosure, loss, alteration, or compromise of identifiable research information must be reported immediately through the applicable SJBSM information-security/privacy process and to the PI; the PI or a designated institutional official shall determine whether IRB reporting is required under the SJBSM IRB reportable-events policy.

External Modules

REDCap External Modules (including nedCAPTCHA 2, described below) are third-party or custom code that extends REDCap's functionality and runs within the platform. No External Module may be enabled on the SJBSM REDCap instance, at the system or project level, without review and approval by the REDCap Administrators, who evaluate each module for information security, data-privacy impact, and ongoing supportability before enabling it. Investigators who need a capability not available in core REDCap should request it through the REDCap Administrators rather than installing or requesting a module directly from a third party.

IP Address Collection and CAPTCHA/Bot Protection

Standard REDCap surveys that do not use the eConsent framework or a third-party CAPTCHA service do not collect participant IP addresses by default. Where the REDCap eConsent framework is activated, REDCap automatically records participant IP address as described in Section 8.

Where a public survey uses a third-party CAPTCHA service, such as Google reCAPTCHA, to deter automated or bot submissions, that service independently collects the participant's IP address and other device or browser signals as part of its own bot-detection process, separate from REDCap itself.

SJBSM uses nedCAPTCHA 2 (v1.1.3), a REDCap External Module that generates CAPTCHA challenges natively within REDCap without relying on an external third-party service. Because nedCAPTCHA 2 does not transmit visitor data to an outside vendor, its use does not introduce the additional third-party IP address collection associated with services such as Google reCAPTCHA. Accordingly, a survey that does not use eConsent and that relies on nedCAPTCHA 2 rather than a third-party CAPTCHA service for bot protection does not collect participant IP addresses through either mechanism.

Investigators must accurately state, in the protocol and consent document, whether participant IP addresses will be collected for a given project, based on whether that project uses the eConsent framework (Section 8) and/or a third-party CAPTCHA service, consistent with the identifiers described in Section 12.

11. Research Data Management and Record Retention

SJBSM requires study records maintained in or generated from REDCap — including REDCap project files, audit trails, data dictionaries, data exports, consent documents (including eConsent records), protocol files, and IRB correspondence — to be retained for at least three (3) years after completion of the research, unless a longer period is required by applicable federal or territorial law, FDA requirements, sponsor terms, funding-agency requirements, the IRB-approved protocol, or another institutional policy. Completion of research means that all research interactions or interventions with participants, and all data collection and analyses involving identifiable information, have ended.

This three-year minimum is an SJBSM institutional records-retention requirement. Records required to be maintained under 45 CFR 46.115 (governing IRB and certain institutional records) must additionally be retained and made available in accordance with that regulation; 45 CFR 46.115 is one component of, and does not by itself establish, SJBSM's broader retention requirement for REDCap research records. The Principal Investigator remains responsible for maintaining secure, access-controlled, and auditable records for the full retention period, including after a project is closed in REDCap.

Data Destruction and Institutional Backups

SJBSM's IT Department maintains routine backups of the REDCap server and its data solely for institutional disaster-recovery and business-continuity purposes — that is, to allow the server and its data to be restored in the event of server failure, system error, or other system-level data loss, including data loss that could occur during a platform update or other maintenance activity. Backups exist for this system-continuity purpose only.

Backup access is controlled exclusively by the IT Department. Investigators and study teams do not have access to backup copies, cannot request retrieval of individual records or projects from backup for research purposes, and cannot use backups as a means of accessing, recovering, or extending access to study data after a project has reached the end of its retention period and been destroyed. Backups exist to protect the institution's systems generally, not to preserve individual study data for research use beyond its approved retention period.

Where a protocol or consent document commits to destroying REDCap project data and locally exported files at the end of the retention period, that commitment must be stated accurately alongside the existence of IT's backups, so the two statements do not appear to conflict.

Protocols and consent documents describing planned data destruction should include language substantially equivalent to the following:

"After the required retention period, the REDCap project and local exported files will be permanently deleted according to institutional data destruction procedures. SJBSM's IT Department separately maintains routine backups of the REDCap server for institutional disaster-recovery purposes only, in the event of server failure or other system-level data loss. These backups are accessible only to IT Department staff; investigators and study teams do not have access to them, and they are not used to retrieve, restore, or provide research access to a study's data after that data has been destroyed. Backup copies are retained and cycled according to IT's own backup schedule, independent of this study's data-retention period."

Investigators should confirm the current IT backup retention/cycling schedule with the REDCap Administrators before finalizing this language in a specific protocol or consent document, so that any stated timeframe is accurate.

12. Guidance for Describing REDCap Use in an IRB Proposal

This section provides investigators with practical guidance for describing REDCap use in the data management, methods, or procedures section of an IRB submission. It draws on the requirements set out in Sections 6 through 11 above and does not restate them in full; it does not replace SJBSM IRB application forms or instructions, and investigators should follow the current IRB application and use the language below only as a starting point to adapt to their specific study.

What to Include

A REDCap data management description should ordinarily address each of the following elements:

- Platform and hosting — state that data will be collected/managed using REDCap, a secure, web-based application hosted by SJBSM, and its intended function in the study (e.g., survey administration, case report forms, eConsent, randomization).
- Data collected — summarize the categories of data to be collected in REDCap (e.g., demographics, clinical measures, survey responses) and whether identifiable or coded/de-identified data will be entered.
- Identifiers and linkage — describe whether direct identifiers (name, medical record number, contact information) will be stored in REDCap and, if so, how they will be separated from research data (e.g., a separate identified instrument, data access groups, or a secure linkage/key file) and who may access the linkage. State whether participant IP addresses will be collected, per the eConsent rule in Section 8 and the CAPTCHA rule in Section 10.

- Access control — describe who will have access to the REDCap project (study team roles) and confirm that access will be limited on a least-privilege, role-based basis consistent with SJBSM Research Center REDCap policy (Section 10).
- Consent process, if applicable — if REDCap eConsent will be used, describe the workflow (how the form is presented, how questions can be asked, how consent is documented, and how a copy is provided to the participant) and confirm the REDCap instrument will match the IRB-approved consent form, per Section 8.
- Recruitment materials, if applicable — describe any REDCap-generated recruitment materials (survey links, QR codes, SMS/email invitations) that will be submitted for IRB review, consistent with Section 9 of this policy.
- Data security — reference the safeguards applicable to the project (e.g., role-based access, audit trails, institutional REDCap security controls) rather than restating Section 10 verbatim.
- Data retention and storage location — state that study data will be retained consistent with SJBSM's REDCap record-retention requirements (Section 11) and any additional sponsor, funder, or regulatory retention periods that apply to the study.
- Secondary use or data sharing, if planned — briefly describe any intended secondary analyses or external data-sharing arrangements, noting that such use may require separate IRB review per Section 13 of this policy.

Sample Language Investigators May Adapt

The paragraph below follows the standard REDCap Consortium citation template published by the REDCap coordinating team and used, with minor institution-specific variation, across REDCap partner sites. Before submission, every bracketed option below must be resolved into plain, specific text describing this study; a submission that still contains bracket punctuation or unresolved alternatives will be treated as incomplete, not merely rough.

"Study data will be collected and managed using REDCap (Research Electronic Data Capture) electronic data capture tools hosted at San Juan Bautista School of Medicine. REDCap is a secure, web-based software platform designed to support data capture for research studies, providing an intuitive interface for validated data entry, audit trails to track data manipulation and export, automated export procedures to common statistical packages, and procedures for integrating data from external sources. Access to the project will be limited to approved study personnel on a role-based, least-privilege basis. [Identifiable information such as name and contact information / No directly identifying information] will be stored in REDCap[, and will be separated from coded research data using (data access groups / a separate identified instrument / other method)]. [This project does not use REDCap eConsent or a third-party CAPTCHA service and will not collect participant IP addresses. / This project uses REDCap eConsent, which will record participant IP address as part of the consent completion record. / This project uses a third-party CAPTCHA service for bot protection, which will independently collect participant IP

address.] Study data will be retained for [at least three years / [longer period specific to this study]] after study completion, consistent with SJBSM Research Center REDCap policy and applicable regulatory and sponsor requirements; after that period, the REDCap project and any local exported files will be permanently deleted according to institutional data destruction procedures. SJBSM's IT Department separately maintains routine server backups for institutional disaster-recovery purposes only; investigators do not have access to these backups, and they are not used to retrieve or restore study data after it has been destroyed."

Where REDCap eConsent will be used, the following structure — adapted from Vanderbilt University Medical Center IRB guidance for REDCap eConsent submissions — is a useful starting point (see Section 8 for the underlying requirements this text is meant to satisfy): "This study will utilize the electronic consent (eConsent) framework within REDCap. The consent form will be presented to the participant (or legally authorized representative) electronically for review, questions, and electronic signature, matching the IRB-approved consent document. Signed consent forms will be archived as PDF records for documentation and future reference. Any subsequent change to the consent form will be submitted to the IRB for approval before it is implemented in REDCap. The information gathered through the electronic process will be equivalent to what would be collected through an in-person, paper-based consent process. As part of this process, REDCap will automatically record the participant's IP address as part of the consent completion record; this collection is disclosed to the participant in this consent document." [For FDA-regulated studies, add a statement addressing 21 CFR Part 11 electronic-record/signature compliance.]

Sources: REDCap Consortium, "Citing REDCap" (projectredcap.org/resources/citations); Vanderbilt University Medical Center IRB, REDCap eConsent submission guidance. Investigators should verify current template language with the REDCap Administrators, as these sources may be updated over time.

Pre-Activation Verification Materials

When the IRB requests final REDCap screenshots or an instrument export before a project is activated in Production Mode, this requirement has two distinct components, and investigators should address both unless the IRB states otherwise for a specific protocol:

- Configuration and content verification — a PDF or data-dictionary export of the finalized instrument(s) showing the exact question wording, response options, and branching/skip logic as they will appear to participants, together with screenshots of the relevant Survey Settings (e.g., confirmation that "Anonymous survey" is enabled where the protocol represents the survey as anonymous, and that IP address, geolocation, and other device metadata collection are disabled where the protocol states they will not be collected). This documents that the live configuration matches what was represented in the IRB-approved protocol and consent materials.
- Functional verification — confirmation that the survey has been tested end-to-end in Development Mode (e.g., a single test entry completed by a study team member) to verify

that branching logic, required fields, and submission behave as intended. Test entries created for this purpose are not participant data, must not contain real participant identifiers, and should be deleted from the project before or immediately upon moving to Production Mode; a brief written confirmation from the study team that functional testing was completed and test data removed is normally sufficient documentation of this step, rather than screenshots of the test submission itself.

In other words: the IRB's request is ordinarily satisfied by (1) the instrument export/settings screenshots described above, plus (2) a short statement confirming the survey was functionally tested and any test data removed — not by a screenshot of every field in the production database after real data collection has begun, and not by retaining a test participant's submitted responses as evidence. Because expectations can vary by protocol, investigators who are unsure what a specific IRB comment requires should ask the IRB Director directly to confirm scope before assembling materials, rather than assuming the broadest possible interpretation.

Common Reasons for IRB Deferral or Clarification Requests

- The submission does not state whether identifiable data will be stored in REDCap or how it will be separated from research data
- The submission does not describe who will have access to the REDCap project or how access will be limited
- An eConsent workflow is referenced but not described, or the REDCap instrument does not match the attached consent form
- Recruitment materials (QR codes, survey links, invitation text) are referenced but not included for review
- No data retention period is stated, or it is inconsistent with SJBSM policy or applicable sponsor/funder requirements
- The submission states that no identifiers will be collected but does not address IP address collection triggered by REDCap eConsent (Section 8) or a third-party CAPTCHA service (Section 10)

Investigators are encouraged to contact the REDCap Administrators for help describing a project's technical configuration (e.g., data access groups, field-level security, survey vs. longitudinal design) and to contact the IRB directly with questions about what a specific submission must include. The REDCap Administrators can advise on technical description but do not determine IRB submission sufficiency.

13. Secondary Use of Data

Use of identifiable data for purposes outside the original IRB-approved protocol — including secondary analysis, data sharing with external collaborators, or use in a new study — may require additional IRB review and approval prior to implementation. Investigators should consult the IRB before repurposing REDCap data collected under a prior approval.

14. Audits and Monitoring

SJBSM reserves the right to audit REDCap projects at any time, including review of user access lists, permission assignments, project logs, audit trails, and supporting compliance documentation. Audits may be initiated by the Research Center or the IRB, and conducted by the IRB, its designees, or the Research Center. The REDCap Administrators support these audits by providing technical records, audit logs, user-rights information, and system assistance, consistent with the REDCap Administrators' role described in Section 5, and do not independently determine compliance outcomes. Audits may be routine, for-cause, or requested in connection with an external sponsor or regulatory inspection.

15. Noncompliance and Reportable Events

Unauthorized data collection, recruitment, or consent activity; use of non-IRB-approved materials; misuse of identifiable data; or other violations of this policy may result in one or more of the following actions:

- Suspension or termination of REDCap access
- Required corrective action plan and/or retraining
- Referral to the IRB for review as a deviation or noncompliance event
- Referral to appropriate institutional compliance, research integrity, or human resources offices

For covered research, SJBSM procedures provide for prompt reporting of: (a) unanticipated problems involving risks to subjects or others; (b) serious or continuing noncompliance with 45 CFR 46 or IRB requirements or determinations; and (c) suspension or termination of IRB approval. As applicable, these events must be reported to the IRB, appropriate institutional officials, the relevant federal department or agency, and OHRP, in accordance with the SJBSM IRB policy governing reportable events. A confidentiality or cybersecurity incident involving REDCap data may constitute an unanticipated problem if it is unexpected, related or possibly related to the research, and suggests greater risk of harm than was previously known; the IRB, not the REDCap Administrators, determines whether an event meets this threshold.

16. Training Requirements

All individuals granted REDCap access must complete institutionally required human subjects' protections training (e.g., CITI Program) and any SJBSM REDCap-specific onboarding provided by the Research Center prior to being granted production-level access. Refresher training may be required following a compliance finding or a significant platform update.

17. REDCap Citation Requirement

Consistent with the terms of the REDCap Consortium license and Vanderbilt University Medical Center governance, any manuscript, abstract, poster, thesis, dissertation, grant report, or other publication or presentation that uses data collected, managed, or exported through the SJBSM REDCap system must cite REDCap in the methods section (or equivalent) and, where applicable, acknowledge institutional REDCap support in the acknowledgments section.

Required Citations

Investigators must cite both of the following primary REDCap publications wherever journal or publisher formatting permits multiple citations:

- Harris PA, Taylor R, Thielke R, Payne J, Gonzalez N, Conde JG. Research electronic data capture (REDCap) — A metadata-driven methodology and workflow process for providing translational research informatics support. *J Biomed Inform.* 2009;42(2):377-381.
- Harris PA, Taylor R, Minor BL, et al. The REDCap Consortium: Building an international community of software partners. *J Biomed Inform.* 2019;95:103208.

Suggested Acknowledgment Language

Where an acknowledgments section is permitted, investigators are encouraged to include substantively the following: "Data for this project were collected and managed using REDCap electronic data capture tools hosted at San Juan Bautista School of Medicine. REDCap is a secure, web-based software platform designed to support data capture for research studies."

The PI is responsible for ensuring citation compliance for all outputs generated from an SJBSM REDCap project and for retaining a copy of the final published or presented material, consistent with the record retention requirements of this policy. The REDCap Administrators can provide the current, institution-specific citation and acknowledgment text upon request.

18. Policy Review

This policy will be reviewed at least every two years, or sooner if required by changes in federal regulation, OHRP guidance, REDCap Consortium terms, or SJBSM institutional policy; the Research Center will issue updates in consultation with the IRB, and the Institutional Research Committee will approve them.

19. Regulatory and Institutional References

- 45 CFR 46 (Common Rule) — Protection of Human Subjects
- 45 CFR 46.104 — Exempt Research
- 45 CFR 46.108(a)(4) — Institutional Reporting Procedures
- 45 CFR 46.109 — IRB Review Authority (approve, require modifications, or disapprove)
- 45 CFR 46.111 — Criteria for IRB Approval
- 45 CFR 46.114 — Cooperative Research; Use of a Single IRB
- 45 CFR 46.115 — IRB Records; Institutional Record Retention Requirements
- 45 CFR 46.116, 46.117 — General Requirements and Documentation of Informed Consent
- OHRP Investigator Responsibilities: Frequently Asked Questions
- OHRP Revised Common Rule: Frequently Asked Questions
- OHRP/FDA Guidance on Electronic Informed Consent
- 21 CFR Parts 11, 50, 56, 312, and 812, as applicable to FDA-regulated research
- HIPAA Privacy and Security Rules
- Vanderbilt University Medical Center REDCap and eConsent Governance Guidance
- REDCap Consortium End-User Agreement
- SJBSM Institutional IRB Policies and Procedures, including the reportable-events policy
- Harris PA, et al. Research electronic data capture (REDCap). *J Biomed Inform.* 2009;42(2):377-381.
- Harris PA, et al. The REDCap Consortium. *J Biomed Inform.* 2019;95:103208.
- Rezniczek, G.A. nedCAPTCHA 2 (REDCap External Module), v1.1.3 — in-platform CAPTCHA protection used in place of a third-party CAPTCHA service.