UNIVERSITY of WASHINGTON
HUMAN SUBJECTS DIVISION

SUPPLEMENT Other REDCap Installation

PURPOSE

The purpose of this supplemental form is to assist HSD staff in determining if the non-UW REDCap installation meets UW criteria for security and reliability for conducting and documenting electronic consent (including compliance with 21 CFR 11 and with Washington State law).

INSTRUCTIONS

For each requirement below, please review and indicate in the far-right column whether the REDCap installation being used for your study meets this requirement. Some requirements may require review by an IT expert who has responsibility/oversight for the system. **All** requirements listed below must be met to use a non-UW REDCap installation for conducting and documenting electronic consent.

Upload the completed Supplement to your Zipline application on the **Study-Related Documents** SmartForm for multi-site studies or the **Local Site Documents** SmartForm for single-site studies.

REDCap TECHNICAL SECURITY CHECKLIST FOR E-SIGNATURE FOR UW IRB	YES	NO
1. Disaster Recovery Plan Does the REDCap installation have a disaster recovery plan in place?	☐	☐
2. Dedicated REDCap Administrator Does the REDCap installation have dedicated REDCap Administrator to handle troubleshooting, access issues, security concerns?	☐	☐
3. Validation before upgrade Is REDCap validated in a development or test environment before upgrading?	☐	☐
4. Validation of External Modules If External Modules are enabled in the REDCap instance, are both the active External Modules and REDCap validated before upgrading? If you did not enable External Modules, answer this question with "Yes".	☐	☐
5. Validation Logs Is a record of all validation efforts and their outcomes maintained?	☐	☐
6. Daily backups or mirrored database Are daily backups performed on the REDCap database or mirrored databases run on two separate machines?	☐	☐
7. Encrypted servers Is REDCap run on encrypted servers?	☐	☐
8. Regular updates REDCap Is the REDCap installation updated to the latest (or close to) the latest version of REDCap at least every 6 months?	☐	☐
9. Regular security updates for webserver/database server Is the webserver and database server updated with security updates at least every 6 months?	☐	☐
10. Local IT Security HIPAA compliance signoff Did the local IT Security department sign off on the REDCap installation as meeting the physical and technical safeguards set forth in the HIPAA Security Rule?	☐	☐
11. Authentication methods Are you using methods other than table-based authentication in your REDCap installation?	☐	☐

12. Base URL of your REDCap installation:

13. Host institution name:

14. Information for the local REDCap administrator/contact:

Name:	
Email:	
Phone:	

Keyword: Consent