eSource Readiness Assessment Form/S

Assessment of eSource (EHR) Systems Used for Storing Source Data During Clinical Trials

About the eSRA Checklist…

This eSRA Form/S allows a site to assess the GCP compliance of their systems that provide data for clinical research. Sponsors and sites will use the assessments to discuss any risks and appropriate solutions.

Investigator Site

Please complete one Form/S form for each system that will be used as the source for data in a clinical trial.

Date of eSRA Completion — Day | Month | Year

Your Institution

Official Institution Name

Official Site Name (*within institution)*

Address line 1

Centre Number *(Optional)*

Address line 2

Site Description

City

State / Region

Postal Code

Country

User Contact Details

Backup User Contact Details

First Name

Last Name

Phone Number (*optional)*

E-mail Address

Role

System Details

System Name: REDCap

Developer/Vendor Company Name: Vanderbilt University

Version Number: 16.1.5

Release Date: Day 05 | Month 03 | Year 2026

Modules applicable to this assessment

Description of System

- ○ Electronic Health Record System (EHRS) or Electronic Medical Record System (EMRS)
- ○ Laboratory/Diagnostic System
- ○ Imaging System (e.g., x-ray, CT scan)
- ○ Pharmacy System (if used to hold records of subject medication dosing)
- ○ Radiology System
- ◉ Other eSource System (specify) Electronic Case Report Form / Clinical Database System

If system is certified by a national authorising body (e.g., the U.S. ONC Health IT Certification Program), list the certification body name, certification name and version, date of certification. Note: If this system becomes decertified, all sponsors must be notified of the reason and this form must be updated.

eSource System Criteria

Please provide an answer for each question in order for the assessment to be considered complete.

Assessment Question	*Investigator Site Response*	*Comment -- If response is "No", additional information and/ or plans to correct deficiencies are required. (Max: 120 char)*

Records for Clinical Research

1. Can all patient records captured in the EHR system be retrieved and reviewed in a way that is attributable to one trial subject?

◉ *Yes* ○ *No **

Note. *ALL patient records do not need to be stored in this system, however all records in the system must be able to be attributed to a particular patient. This is NOT about linking to a clinical patient ID, but rather about being sure that all records are attributable to an individual.*

2. ^ Are all records given to the sponsor via electronic or manual means de-identified, such that they do not contain any patient-identifiers that are prohibited by the country in which the clinical trial is taking place?

◉ *Yes* ○ *No*

Sponsor's responsibility at project level.

Note. *If access to an electronic site system by a sponsor/CRO results in files being automatically downloaded to their laptop, the answer to this question would be "no". It is not permissible for personal health information to be downloaded (even inadvertently) to a sponsor/CRO personal computer.*

Audit Trail

3. Does the system have a readable, readily available, and indelible audit trail to include recording date/time/originator?

◉ *Yes* ○ *No **

Note. *Site must ensure that audit trail (audit log) functionality has been installed and is working correctly. If an appropriate audit trail is not available, additional process controls, such as a signed and dated print out, will have to be introduced to maintain the information.*

4. Does the audit trail include the reason for change of any trial participant data change or deletion if this is legally required in your region?

◉ *Yes* ○ *No ** ○ *N/A*

Possible, but must be enabled in the individual project. REDCap also offers a Data Resolution Workflow for monitoring.

Note. *If an appropriate audit trail is not available, additional process controls, such as a signed and dated print out, will have to be introduced to maintain the information.*

5. Are there processes and/or system controls in place that prevent the modification of the audit trail or turning off the audit trail or changing system date/time?

◉ *Yes* ○ *No*

It is not possible for users to delete or change the audit trail.

Note. *This may be handled via the site operating system and associated procedures or via a hosting vendor. The site should ensure the method employed is working.*

6.^ Does the system and/or process adequately provide for identifying the local time of patient events?

◉ *Yes* ○ *No* ○ *N/A*

Note. *Where the system use may span time zones or the system may be located in a different time zone than where the study is being conducted, the time zone of the investigative office (e.g., local time to the patient) should be used in the audit trail, or there must be a clearly documented consistent way to derive the local time from the timestamp on the audit trail.*

Assessment Question	Investigator Site Response	Comment -- If response is"No", additional information and/ or plans to correct deficiencies are required. (Max: 120 char)

Access Control

7. Does the system have the ability to create, maintain, apply and revoke the roles, access permissions and capabilities of each user that accesses the system, such that users have access only to those system functions and data that are appropriate to their role?

(●) Yes ( ) No *

Users are granted access to a REDCap project with specific rights and data access. Role-based access is possible.

Note. *Sites must ensure that accounts are configured so that users have access to only those features that they should have access to (often referred to as roles). Also, there should be an administrator to grant accounts to users upon justification of their need for an account. A process should be in place to ensure that access is removed when an employee no longer has justification for using the system (such as getting assigned to a different area or leaving the organisation). If you are using a hosted system, be sure that the vendor will provide the user administration and that you understand and employ the process for obtaining and removing accounts.*

8. Is there a process to periodically produce and review a list of all users, including past users, their access level/rights and the start and end date of these access rights?

(●) Yes ( ) No *

Note. *The site personnel log should also include other non-site persons who may have access to the clinical study/trial electronic source data. This report does not have to be kept by the investigator, but should be available, upon request, from the IT department or vendor which maintains the system.*

9. Is there a policy/procedure/training that each account is assigned to one dedicated user and that instructs users not to share their account or to leave their account open for others to use?

(●) Yes ( ) No

All staff complete a compulsory e-learning course on information security.

10.^ Can the monitor, auditor and inspector, within reasonable timeframe, obtain direct read-only access to records of only subjects of this clinical trial?

(●) Yes ( ) No*

Note. *The investigator (or appropriate delegate) should be available to browse the patients' record on demand in case of audit, inspection or for monitoring purpose. It is recommended this requirement be part of the contract between the sponsor and the investigator (or the study center). If you are under the jurisdiction of MHRA, please see additional information in Section 3.4 of the eSRA Handbook.*

11. ^ Is there a documented site procedure in place to ensure clinical trial staff are not unintentionally unblinded in trials where this is a requirement?

(●) Yes ( ) No ( ) N/A

Possible, but must be enabled in the individual project.

Note. *If your site does now or may in the future handle blinded studies, this question must be answered. For example, information on pharmacy distribution should not be available for study staff to see.*

12. Is there a limited number of unsuccessful log-in attempts permitted by the system?

(●) Yes ( ) No *

Users log in with Shibboleth, i.e. with their Citrix account, so multiple attempts are not possible.

Note. *An example of an unsuccessful log-in attempt is a forgotten password. This may be handled via the site operating system and associated procedures or via the EHR system. Site must ensure that this feature is installed and turned on.*

13. Does the system keep a log of unauthorised access attempts and is there a process in place to periodically review the log of unauthorised access attempts?

(●) Yes ( ) No

Note. *An example of an unauthorised access attempt is a hacking attempt.This may be handled via the site operating system and associated procedures or via the EHR system. Site must ensure that this feature is installed and turned on.*

14. Does the system require secure access via (check all that apply)

Citrix password is changed every 6 months

- [x] Require password change (indicate interval in the comment block)
- [ ] Fingerprint
- [ ] Face Recognition
- [x] Device (e.g. smartphone code)
- [ ] Single Sign-on
- [ ] Same Sign-on
- [ ] Other

Note. *Site must ensure that this feature is installed and turned on. If access is provided via a password, site is responsible for establishing reasonable intervals. If managing password updates via a process, the site must provide and enforce a documented site process requiring password change.*

15. Is there a process that in case of security incident that exposes privacy data, the sponsor and relevant data protection supervisory authority are notified?

(●) Yes ( ) No *

16. Is there an automatic log-off or other access lock (e.g., password protected screen saver) after a period of inactivity? If "yes", please indicate in the comment block the period of inactivity before the automatic log-off.

(●) Yes ( ) No *

Citrix users are logged out after 20 minutes idle time.

Note. *Site must ensure that this automatic feature is installed and turned on. If using password protected screen-saver function from your laptop or desktop system to satisfy this requirement, users should not have the ability to turn off the password-protected screen saver functionality.*

Assessment Question	Investigator Site Response	Comment -- If response is "No", additional information and/ or plans to correct deficiencies are required. (Max: 120 char)

Data Review

17. Does the system have the ability to produce a copy of data (which includes associated audit trails and any decoded data) in appropriate file format that facilitates review, searching and analysis?

- (●) Yes
- ( ) No

Data and audit trail in two separate files (.csv)

Note. *If your system does not provide this, a documented site process should address how a certified copy could be produced.*

Data Backup, Retention and Recovery

18. Are there sufficient system and/or process controls for backup and recovery procedures, that includes documentation that can be produced for inspection by a monitor, auditor or inspector?

- (●) Yes
- ( ) No *

Note. *This may be handled via the site operating system and associated procedures or via the eSource system.*

19. Are there process or system controls in place to ensure that data and metadata (including audit trail) continue to be available, human-readable and understandable and are retained in an archive for the legal period?

- (●) Yes
- ( ) No *

Note. *Sites are responsible for knowing the legal retention period for clinical research source records and for ensuring that methods employed to meet this requirement are working.*

20. Is there a documented process for continuing operations if the system is not accessible?

- ( ) Yes
- (●) No

In case of downtime, users are responsible to write down data and enter it later. Forms can easily be downloaded in pdf

Note. *There should be a documented site process/plan describing how to handle an emergency or unexpected shutdown. The site should have access to these documents. The site should confirm and request immediate remediation if there is nothing already in place and/or if the process has not been tested.*

21. Is there a documented and tested process for recovery from a disaster or unexpected system unavailability?

- (●) Yes
- ( ) No

Note. *The group responsible for backup and recovery of the system software/hardware (whether it is your IT department or a vendor) should have a documented site process describing how recovery from an emergency or unexpected shutdown will be handled and proof that this process was tested. The site should have access to these documents.The site should confirm and request immediate remediation if there is nothing already in place and/or if the process has not been tested.*

System Development & Maintenance

22. ^ Are there documented records showing that those maintaining or using the system are qualified (have the necessary training and experience to be able to perform their assigned tasks)?

- (●) Yes
- ( ) No

23. Does the site utilise a process to demonstrate that the development, hosting, deployment and maintenance (e.g. system changes) of the computerised system is sufficiently validated and documented?

- (●) Yes
- ( ) No *

Note. *When purchasing or upgrading software, it is typical to have a list of requirements for what it should do and then test to see that it does perform those functions. Validation is a formalization of this process and good business practice. Validation is only required for the parts of the system (modules) necessary to comply with clinical research requirements. All validation/testing activities should be documented such that they can be audited by the sponsor or inspected by a regulatory agency. If the system is upgraded to a new version the changes might require validation, depending on the extent and the scope of the changes. The site must keep track of what version of the system was in place on what date.*

24. Are there processes to address computerised system incidents through to their resolution?

- (●) Yes
- ( ) No

25. Is there a process to periodically review and affirm the continued suitability of the computerised system taking into account the potential cumulative risks and impacts of changes to the system, requirements, version releases, and computing environment of the system?

- (●) Yes
- ( ) No

26. Are there sufficient information security practices to manage, preclude, and report security issues?

- (●) Yes
- ( ) No

Note. *This may be handled via the site operating system and associated procedures. The site should ensure the method employed is working and documented. Site should check with their IT support that cyber security measures are in place and updated regularly.*

27. If electronic data is received from other systems (internal or external), are there appropriate technical or procedural controls to assure confidentiality and integrity of data received from these systems?

- (●) Yes
- ( ) No
- ( ) N/A

Assessment Question	Investigator Site Response	Comment -- If response is "No", additional information and/ or plans to correct deficiencies are required. (Max: 120 char)

28. ^ If this computerised system is provided by a Service Provider, are there formal agreements in place to clearly define 1) responsibilities of each party (Site and Service Provider and Service Provider's GxP-related subcontractors) and 2) oversight of the Service Provider?

- (●) *Yes*
- ( ) *No*
- ( ) *N/A*

Service Level Agreement (SLA) med RM IT

Note. The department responsible can achieve this by an appendix to the contract, an SLA (Service Level Agreement), or in a "statement of work" that can be downloaded from the vendor website.

29. If electronic signatures are used in this system to fulfill clinical research requirements, are all of the following true: 1) it is permanently linked to its respective record, 2) it includes the name of the signer, 3) it includes the time and date of e-signature execution, 4) the meaning associated with the e-signature is indicated (e.g., creation, confirmation, approval), 5) system can recognise if a record has been altered and make the signature invalid.

- ( ) *Yes*
- (●) *No **
- ( ) *N/A*

REDCap does not offer eIDAS compliant digital signatures. Informed consent can be done in xFlow.

Note. There is no requirement that electronic signatures are used unless expressly indicated in the protocol. The electronic signature can take various forms, including digital signature, as long as they are legally valid within the jurisdiction where the research is to be conducted.

ADDITIONAL INFORMATION

Additional Comments from Site

The shared workspace for all staff in the Central Denmark Region is built on Citrix Virtual Apps and Desktops. There is full central control, management, software deployment and patching.The operating system is Windows 11 Enterprise with continuous virus protection by Microsoft Defender for Endpoint.

I have assessed this completed document and I accept the risks and mitigations identified in this document as per ICH E6 R3 2.12.10 and 3.16.1.vi and vii.

Principal Investigator signature and date

*** Based on clinical research regulations and guidances, it is strongly recommended to mitigate this item, dependent on the nature of the study, prior to using eSource from this system..**

^ indicates a process question that must be answered if the site is using a previously completed eSRA or Form/S from another part of their organisation.

Instructions and License Agreement pertaining to this Assessment can be found in the eSRA Handbook which can be downloaded from https://eclinicalforum.org/site-sys-assts.

