Instructions:

- *This checklist is to be used as an internal tool and is optional for completion for electronic information systems used in the conduct of NIAID DAIDS Network studies conducted within the Clinical Trials Networks.*
- *This checklist may be completed by the entity that owns/implements the system. Please utilize available reference resources including the Electronic Information Systems Policy and Appendix A, Requirements for using Electronic Information Systems in Clinical Research for additional information.*
- *This checklist is an optional internal tool that may be completed for all new electronic information systems and for all subsequent software release versions of the system. The checklist serves as a guide to capture important information about the electronic system and does not replace validation documentation requirements.*

Site Information	
Date of Submission:	DD-Mon-YYYY
Site Number (if applicable):	Specify here. Enter N/A if Site Number is not applicable.
Site/Organization Name:	Specify here.
Site/Organization Contact Name:	Specify here.
Site/Organization Contact Phone:	Specify here.
Site/Organization Contact Email:	Specify here.

System Information	
Name of System being Assessed: Specify here.	
System Version #: Specify here. *Note: Ensure System Version and Date of Implementation are in alignment if applicable.	**Date of Implementation:** DD-Mon-YYYY *Note: Ensure System Version and Date of Implementation are in alignment if applicable.
Describe the ***purpose*** of the system:	Enter specific information here about the system including system type (e.g., web application). Describe how the system will be used in support of the Clinical Trials Networks.
Describe the ***process*** surrounding the use of the system:	Enter information here about the process for the use of this system. Describe the business use of the system by defining the business-critical functions that the system performs (e.g., what needs the system address, what regulations the system helps the business meet, what benefits are gained).

System Information		
Vendor Name:	Specify here.	***Software Acquisition:*** ☐ Purchased Software (Run/Installed locally) ☐ In-House/Custom Developed Software ☐ Software as a Service (SaaS)
System Contact Person:	Specify here.	
Other Information:	Enter any additional information here that may be important to know about the system that is not captured in any of the existing sections. Enter N/A in this field if there are no additional comments to be entered.	

Determining System Validation Scope
• *Utilize Section 1.0 to determine the validation scope of the electronic information system being used within the Clinical Trials Networks according to the regulations and your site or organization's procedures.*

Section 1.0 Determination of Validation Scope		
1.1	Does the system generate, capture, process, report, store, or archive raw and/or source data or records?	☐ Yes ☐ No
1.2	Will the data or records from this system be submitted as part of required periodic (e.g., annual) study reports?	☐ Yes ☐ No
1.3	Will the data or records from this system be part of a final clinical study report (CSR)?	☐ Yes ☐ No
1.4	Would the data or records, such as essential documents, from this system be required to reconstruct a trial?	☐ Yes ☐ No
1.5	Could participant safety be impacted from decisions made using incorrect or inaccurate data or records from this system?	☐ Yes ☐ No
1.6	Could participant safety be impacted from other systems processing incorrect or inaccurate data or records from this system?	☐ Yes ☐ No
Based on organizational procedures and regulations use the information in Section1.0 to begin determining the validation needs and scope of the electronic system. Proceed to Section 2.0.		

Electronic Records Requirements

Section 2.0 Validation

2.1	Has this system been validated by your office according to in-house computer system validation procedures?	☐ Yes ☐ No ☐ N/A
2.2	If the system has been validated by your office, is the validation documentation available for review, if required, during a regulatory inspection?	☐ Yes ☐ No ☐ N/A
2.3	Has the vendor validated the system according to the vendor's computer system validation procedures?	☐ Yes ☐ No ☐ N/A
2.4	If the vendor has validated the system, can they provide you with a validation certificate or a similar documentation?	☐ Yes ☐ No ☐ N/A
2.5	If the vendor has validated the system, will they make the validation documentation available for review, if required, during a regulatory inspection?	☐ Yes ☐ No ☐ N/A

Note: If any of the answers above are "No", consider what mitigations of this risk are possible. Consider some type of documented testing with objective evidence to prove at a minimum the functions being used to support the clinical study are working accurately and consistently.

Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.

Section 3.0 Electronic Records Controls

3.1	Is the system able to produce accurate and complete copies of the data/records contained within the system (e.g., on paper)?	☐ Yes ☐ No ☐ N/A
3.2	Is the system able to provide the information in an electronic format (e.g., Excel file, .csv, .xml or similar data extract)?	☐ Yes ☐ No ☐ N/A
3.3	Is the necessary equipment available to place the electronic data/records on an encrypted universal serial bus (USB) drive or other media if required by the regulatory authority?	☐ Yes ☐ No ☐ N/A

Note: If any of the answers above are "No", consider what mitigations of this risk are possible.

Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.

Section 4.0 Protection of Records (applicable for locally run/installed and SaaS systems)

4.1	Are the data/records readily retrievable throughout the retention period?	☐ Yes ☐ No ☐ N/A
4.2	Are the data/records backed up regularly and maintained in a separate location (e.g., alternate clinical site, another location, cloud storage) for disaster recovery purposes?	☐ Yes ☐ No ☐ N/A

Section 4.0 Protection of Records (applicable for locally run/installed and SaaS systems)		
4.3	Is a disaster mitigation and recovery plan in place and regularly reviewed?	☐ Yes ☐ No ☐ N/A
4.4	Are the data/records protected using a firewall?	☐ Yes ☐ No ☐ N/A
4.5	Have firewall rules been defined by the site/organization?	☐ Yes ☐ No ☐ N/A
4.6	Are firewall rules and setting periodically reviewed?	☐ Yes ☐ No ☐ N/A
4.7	Is anti-virus software installed to prevent, detect, and mitigate the effects of viruses, malware, and other harmful software?	☐ Yes ☐ No ☐ N/A
4.8	Is the anti-virus software continuously monitored and updated with the most recent virus definitions?	☐ Yes ☐ No ☐ N/A
4.9	Are relevant security patches for platforms and operating systems applied in a timely manner according to vendor recommendations?	☐ Yes ☐ No ☐ N/A
4.10	Is penetration testing conducted at regular intervals for internet facing systems?	☐ Yes ☐ No ☐ N/A
4.11	Has an intrusion detection and prevention system been implemented on internet facing systems?	☐ Yes ☐ No ☐ N/A
4.12	Have security incident management procedures been defined including reporting, criticality assignment, and corrective and preventive action implementation?	☐ Yes ☐ No ☐ N/A
4.13	Have interfaces between systems (e.g., transfer of data from one system to another) been clearly defined and validated?	☐ Yes ☐ No ☐ N/A
Note: If any of the answers above are "No", consider what mitigations of this risk are possible. Consider when/if keeping paper records might be necessary if systems are not adequately protected. Add a strong virus protection software to the computer system if possible. Ensure information is available to reconstruct source documentation for regulatory inspection and be prepared to describe how data was obtained and managed to prove the integrity of the data. Document changes made to any systems and carefully evaluate the effects of those changes.		
Risk Mitigations/Comments:	Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.	

Section 5.0 Access Control of Records		
5.1	Does the system ensure that only authorized individuals can use it, electronically sign records, alter records, or perform other operations as required?	☐ Yes ☐ No ☐ N/A
5.2	Does the system prompt for an individual's login account and password to prevent unauthorized users from accessing data/records?	☐ Yes ☐ No ☐ N/A

Section 5.0 Access Control of Records		
5.3	Are controls in place to maintain the uniqueness of the user ID and password so that no individual can have the same combination?	☐ Yes ☐ No ☐ N/A
5.4	Is a process in place to promptly remove access upon the departure of an internal employee or upon notification of staff departures from external entities/users?	☐ Yes ☐ No ☐ N/A
5.5	Are requests for access approved and documented?	☐ Yes ☐ No ☐ N/A
5.6	Are users granted the fewest privileges and access rights (least-privilege rule) for them to undertake their specific job duties for as short a time as necessary?	☐ Yes ☐ No ☐ N/A
5.7	Are user accounts traceable to a named user (e.g., no generic or shared accounts)?	☐ Yes ☐ No ☐ N/A
5.8	Are periodic user access and privilege review procedures in place that include but are not necessarily limited to ensuring only necessary and approved users have access, their roles and permissions are appropriate, and their access is promptly removed when no longer necessary or permitted?	☐ Yes ☐ No ☐ N/A
5.9	Are processes in place to deactivate lost, stolen, missing or otherwise compromised IDs, tokens, cards, etc. that are used for access and/or electronic signature purposes?	☐ Yes ☐ No ☐ N/A
5.10	Are processes in place for initial and periodic testing of IDs, tokens, cards, etc. that are used for access and/or electronic signature purposes?	☐ Yes ☐ No ☐ N/A
5.11	Is there a process to ensure the recalling of IDs, tokens, cards, etc. if a person leaves employment or is transferred to a different job role?	☐ Yes ☐ No ☐ N/A
5.12	Does the system have safeguards to prevent unauthorized use of passwords and/or identification codes?	☐ Yes ☐ No ☐ N/A
5.13	Is there a process in place to immediately detect and report attempts at unauthorized use of passwords and/or identification codes?	☐ Yes ☐ No ☐ N/A
5.14	Have password policies been implemented that include but are not necessarily limited to, length, complexity, expiry, login attempts, and logout reset?	☐ Yes ☐ No ☐ N/A
5.15	Have the password policies been verified and documented as part of the system validation?	☐ Yes ☐ No ☐ N/A
5.16	Are individual accounts password protected?	☐ Yes ☐ No ☐ N/A
5.17	Are passwords required to be reset at some set periodic interval?	☐ Yes ☐ No ☐ N/A
5.18	Is the system setup with an automatic inactivity logout to log out users after a defined period of inactivity?	☐ Yes ☐ No ☐ N/A
5.19	Is the system setup to prevent the average user from setting the inactivity timeframe or deactivating the functionality?	☐ Yes ☐ No ☐ N/A

Section 5.0 Access Control of Records		
5.20	Does the system limit the number of failed login attempts?	☐ Yes ☐ No ☐ N/A
5.21	Is the system available with full, direct, and read-only access (this requires a unique identification method e.g., username and password) upon request by inspectors from regulatory authorities?	☐ Yes ☐ No ☐ N/A
Note: If any of the answers above are "No", consider what mitigations of this risk are possible. Implementing a procedure that is followed to onboard or offboard and employee is one way to mitigate risks regarding control of access. A procedure to train individuals on protecting their accounts is also recommended to include: 1. Do not share individual account access with other users, 2. Do not log on to a system to provide access for another user, 3. Require users to change passwords at regular intervals, and 4. Automatically lock computers when left idle for a short period of time.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

Section 6.0 Audit Trails		
6.1	Does the system have an audit trail to track user entries and actions that create, modify, or delete data/records? *Note: if answered No or N/A, all other answers in this section will be N/A.*	☐ Yes ☐ No ☐ N/A
6.2	Does the audit trail keep copies of deleted records?	☐ Yes ☐ No ☐ N/A
6.3	Does the audit trail ensure that the previously recorded information is still available (i.e., not obscured by the change)?	☐ Yes ☐ No ☐ N/A
6.4	Does the audit trail contain a timestamp that is applied automatically?	☐ Yes ☐ No ☐ N/A
6.5	Does the audit trail track changes in a consistent time zone (e.g., Coordinated Universal Time (UTC))?	☐ Yes ☐ No ☐ N/A
6.6	Does the audit trail keep track of the individual user, including system administrators, who made the change?	☐ Yes ☐ No ☐ N/A
6.7	Is the audit trail protected from modification and deletion by any user, including system administrators?	☐ Yes ☐ No ☐ N/A
6.8	Is it possible to discern invalid or altered records?	☐ Yes ☐ No ☐ N/A
6.9	Is the audit trail available for review throughout the data/record's retention period?	☐ Yes ☐ No ☐ N/A
6.10	Is the audit trail stored within the system itself?	☐ Yes ☐ No ☐ N/A

Section 6.0 Audit Trails		
6.11	Is the audit trail in human-readable format that is comprehendible?	☐ Yes ☐ No ☐ N/A
6.12	Is the audit trail visible at the data-point level in the live system?	☐ Yes ☐ No ☐ N/A
6.13	Is it possible to export the entire audit trail as a dynamic data file (e.g., into an Excel workbook versus as a PDF)?	☐ Yes ☐ No ☐ N/A
6.14	Have audit trail review procedures been put in place that include documentation of the reviews?	☐ Yes ☐ No ☐ N/A
Note: If any of the answers above are "No", consider what mitigations of this risk are possible. For an audit trail to be compliant it must meet all the above criteria. Consider a change log with needed details if components of the above audit trail requirements are missing.		
Risk Mitigations/Comments:	Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.	

Section 7.0 Operational Checks		
7.1	Is the computer system date and time synchronized to an international standard setting source (e.g., UTC)?	☐ Yes ☐ No ☐ N/A
7.2	Does the system limit a user's ability to change date or time?	☐ Yes ☐ No ☐ N/A
7.3	Does the system include year, month, day, hour, minute, and time zone in time stamps?	☐ Yes ☐ No ☐ N/A
7.4	Does the system have checks to ensure steps are performed in the correct order if the sequence of system steps or events is important?	☐ Yes ☐ No ☐ N/A
7.5	Does the system contain checks to identify invalid values and alert the user?	☐ Yes ☐ No ☐ N/A
7.6	Does the system prevent default data entries or automatic duplication of data? (N/A if system is programmed to do so)	☐ Yes ☐ No ☐ N/A
Note: If any of the answers above are "No", consider what mitigations of this risk are possible. Procedures to ensure users know the order of tasks can help mitigate risks regarding this requirement. Consideration may also be given to documenting all date and time changes made to the computer including when changes are made for daylight savings time. Also consider documenting time zone references and naming conventions in the study and validation documentation.		
Risk Mitigations/Comments:	Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.	

Section 8.0 Device Checks		
8.1	Does the system track which device or piece of equipment was used to capture the data (e.g., vital sign, ECG)? This applies only when more than one device is available for use.	☐ Yes ☐ No ☐ N/A
Note: If the answer above is "No", consider what mitigations of this risk are possible. Consider recording this information in a comment on the record or some type of log.		
Risk Mitigations/Comments:	Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.	

Section 9.0 Training		
9.1	Do the individuals that develop, maintain, and/or use the system have sufficient education, training, and experience to perform their assigned tasks?	☐ Yes ☐ No
9.2	Is system training documented?	☐ Yes ☐ No
Note: If any of the answers above are "No", consider what mitigations of this risk are possible. Provide training on the operation and use of the system and document that the training occurred. Conduct training sessions as needed to ensure new personnel are adequately trained as they come on board.		
Risk Mitigations/Comments:	Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.	

Section 10.0 System Documentation		
10.1	Is the distribution of, access to, and the use of systems operation and maintenance documentation controlled?	☐ Yes ☐ No ☐ N/A
10.2	Are there revision and change control procedures established to maintain an audit history that documents time-sequenced development and modification of system documentation?	☐ Yes ☐ No ☐ N/A
10.3	Have procedures been put in place to ensure that the computerized system is used correctly?	☐ Yes ☐ No ☐ N/A
Note: If any of the answers above are "No", consider what mitigations of this risk are possible. Ensure documentation contains a revision history to identify changes made and keep copies of all published versions of the documentation.		
Risk Mitigations/Comments:	Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.	

Section 11.0 Controls for Open Systems		
11.1	Are the data (at rest) encrypted on the storage device?	☐ Yes ☐ No ☐ N/A
11.2	Are the data (in motion) encrypted throughout the process of managing and/or transmitting the data?	☐ Yes ☐ No ☐ N/A
Note: If any of the answers above are "No", consider what mitigations of this risk are possible.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

Section 12.0 Electronic Signature Policy		
12.1	Is there a formal policy for internal systems that ensures individuals are held fully accountable and responsible for actions initiated under their electronic signatures?	☐ Yes ☐ No
Note: If the answer above is "No", consider what mitigations of this risk are possible. Consider writing a policy or adding language to your onboarding documents that must be accepted by the employee.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

Electronic Signature Requirements

Section 13.0 Electronic Signature Determination		
13.1	Does the system use electronic signatures?	☐ Yes ☐ No
Question answered **No**: This is the end of this section. Question answered **Yes**: Proceed to **Section 14.0 Electronic Signature Certification**.		

Section 14.0 Electronic Signature Certification (for internal staff users only)		
14.1	Have plans been submitted in writing to use electronic signature to the FDA?	☐ Yes ☐ No

Section 14.0 Electronic Signature Certification (for internal staff users only)
Note: If the answer above is "No", consider what mitigations of this risk are possible. Consider submitting the non-repudiation agreement by using the sample letters provided by the FDA. The Letter of Non-Repudiation Agreement can be sent to ESG Help Desk at ESGHelpDesk@fda.hhs.gov or a physical copy can be sent to: Electronic Submissions Gateway U.S. Food and Drug Administration 3WFN, Room 7C34 12225 Wilkins Avenue Rockville, MD 20852
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.

Section 15.0 Identity Verification		
15.1	Is there a process in place to verify the identity of the individual before providing them the ability to sign electronically?	☐ Yes ☐ No
Note: If the answer above is "No", consider what mitigations of this risk are possible. Establish a process for verifying identity and consider including this process in the account management policy/procedure.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

Section 16.0 Electronic Signature Uniqueness		
16.1	Are electronic signatures unique to an individual?	☐ Yes ☐ No
16.2	Is there a process in place to ensure electronic signatures are never reused by or reassigned to anyone else?	☐ Yes ☐ No
Note: If any of the answers above are "No", consider what mitigations of this risk are possible. Establish a user account management policy or procedure to ensure user identifications (IDs) are not reused and consider including that if a person is rehired that they should receive the same user ID assigned previously to ensure an individual does not have more than one electronic signature representation.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

Section 17.0 Electronic Signature Components		
17.1	Does the signature require the use of at least two components (i.e., a user ID and password or an ID card and pin number)?	☐ Yes ☐ No

Section 17.0 Electronic Signature Components		
17.2	Does the system prompt for a re-entry of the password or pin upon each application of the electronic signature?	☐ Yes ☐ No
17.3	Does the system prompt for both components (i.e., a user ID and password or an ID card and pin number) when the signing is not performed during a single, continuous period of controlled system access?	☐ Yes ☐ No
17.4	Is there a process in place to ensure electronic signatures are only used by their genuine owners?	☐ Yes ☐ No
17.5	Are electronic signatures administered and executed in a way that requires collaboration of at least two individuals if an attempt is made to falsify a signature?	☐ Yes ☐ No
Note: If any of the answers above are "No", consider what mitigations of this risk are possible. Consider a policy that assures user IDs and passwords are not shared and that users properly log out upon completion of their work particularly if they are using shared workstations.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

Section 18.0 Electronic Signature Elements		
18.1	Does the signed electronic record contain the printed name of the signer?	☐ Yes ☐ No
18.2	Does the signed electronic record contain the date and time of the signing (including time zone) (e.g., UTC)?	☐ Yes ☐ No
18.3	Does the signed electronic record contain the meaning of the signature that was applied (e.g., approval, review)?	☐ Yes ☐ No
18.4	Is the electronic signature and all three (3) of its components (printed name of signer, date and time of signing, and meaning of signature) available for viewing when the electronic record is shown in human readable format (e.g., on an electronic display screen or on a report)?	☐ Yes ☐ No
Note: If any of the answers above are "No", consider what mitigations of this risk are possible.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

Section 19.0 Electronic Signature Linking		
19.1	Are the electronic signatures linked to their respective electronic records to ensure that the signatures cannot be removed, copied, cut and pasted, or transferred by ordinary means in order to falsify an alternate electronic record?	☐ Yes ☐ No

Section 19.0 Electronic Signature Linking		
19.2	Are handwritten signatures applied to electronic records linked in a manner that ensures that the signature cannot be removed, copied, or transferred to falsify an alternate electronic record?	☐ Yes ☐ No ☐ N/A
Note: If any of the answers above are "No", consider what mitigations of this risk are possible.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

Section 20.0 Biometric Electronic Signatures		
20.1	Is there a process in place to ensure that electronic signatures based on biometrics can only be used by their genuine owners?	☐ Yes ☐ No ☐ N/A
Note: If the answer above is "No", consider what mitigations of this risk are possible. Ensure any biometric that may be used (e.g., fingerprints, retinal scans) are truly unique to the individual.		
Risk Mitigations/Comments: Use this section to provide risk mitigations that have been put in place or additional supporting comments. Enter N/A in this field if there are no mitigations or comments to be entered.		

REVISION SUMMARY

1. DAIDS-OD-A-GUD-00005 rev 01, is DAIDS-OPC-A15-GUD-00006 rev 02. This procedure has been transferred from the OPC policy number to a new OD policy document number. DAIDS-OD-A-GUD-00005 is the first revision of this procedure in MasterControl. The document numbering and document format have been updated to reflect current requirements. Instructions were revised to make it optional to submit the checklist.