

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

**Instructions:**

- *This checklist outlines the minimum requirements for an electronic system. This checklist or an equivalent document which contains all the elements from this document on 21 CFR 11 Compliance Risk Assessment must be completed for each electronic system used in the conduct of NIAID DAIDS Network studies conducted within the HIV/AIDS Clinical Trials Networks, unless otherwise specified in a formal agreement. Electronic systems which fall under the scope of this checklist include systems from which clinical trial data may be submitted to the FDA, EMA or any other regulatory authorities.*
- *The checklist should be completed by the entity that owns/implements the system. The checklist must be completed for any new electronic system and for all subsequent software release versions of the system.*
- *When completing this checklist information should be entered in each field that contains blue text prompts and each Yes or No checkbox should be clicked as appropriate to answer each question. Comments may also be entered to provide additional information for mitigation of risk.*

**Points to consider when completing this checklist:**

We recommend that the IT Personnel completing this checklist work with the CRS Leader, or Investigators of Record or Site PI as applicable to determine the applicability of the electronic system.

1. Does the electronic system collect data that will be submitted to any regulatory authority?

**Examples:**

- a. *Will the data be submitted as part of required periodic (e.g. annual) study reports?*
  - b. *Will the data be part of the end of study reports?*
  - c. *Will the data be part of a final clinical study report (CSR)?*
2. Would the records, such as essential documents, be required to reconstruct the trial?  
(See appendix for examples of essential documents)

***If the answer to any of the questions above is 'yes', then you must complete this checklist.***

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

Site Number (if applicable):	
Site Name:	
Contact Name:	
Contact Phone:	
Contact Email Address:	

<b>Name of Electronic System being Assessed:</b>	
--	--

System Risk Assessment	
<b>System Version #:</b>	
Briefly describe the <b>purpose</b> of the system:	
Briefly describe the <b>process</b> surrounding the use of the system: _	
<b>System Acquisition Information:</b>	<b>Software Acquisition:</b> <input type="checkbox"/> Purchased Software (run locally) <input type="checkbox"/> In-House Software/Other <input type="checkbox"/> Software as a Service (SaaS)
<b>System Contact Person</b>	<b>Date of Implementation:</b>
<b>Other Information:</b>	

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: APP-A15-OPC-006.00

**Electronic Records Requirements**

Section 1.0 Validation		
1.1	Has this system been COTS validated by your office?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
1.2	Has the vendor validated the system?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
1.3	If the vendor has validated the system, can they provide you with a validation certificate or a similar documentation?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
1.4	If the vendor has validated the system, will they make the validation information available, if required, during a regulatory inspection?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<p><b>Possible Risk Mitigations and Corrective and Preventive Action (CAPA):</b> If any of the answers above are “No” then you should consider what mitigations of this risk are possible. You should consider some type of documented testing with objective evidence to prove at a minimum the functions you are using to support the clinical study are working accurately and consistently.</p>		
<p><b>Additional Risk Mitigations:</b></p>		

Section 2.0 Access and Controls		
2.1	Is the system able to produce an accurate and complete copy of the records on paper?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
2.2	Is the system able to provide the information in an electronic format (e.g. Excel file, .csv, .xml or similar data extract)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
2.3	Do you have access to equipment necessary to place the electronic data on an encrypted universal serial bus (USB) drive or other media if required by the regulatory authority?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<p><b>Possible Risk Mitigations and Corrective and Preventive Action (CAPA):</b> If any of the answers above are “No” then you should consider what mitigations of this risk are possible.</p>		
<p><b>Additional Risk Mitigations:</b></p>		

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: APP-A15-OPC-006.00

**Section 3.0 Protection of Records (applicable for locally installed and web-based systems)**

3.1	Are the data readily retrievable through the retention period?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
3.2	Are the data backed up to an alternate media on a regular basis and maintained in a separate location (e.g. alternate clinical site, another location, cloud storage, etc.) for disaster recovery purposes?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
3.3	Are the data protected using a firewall?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
3.4	Is the system set up to prevent, detect and mitigate the effects of viruses, malware, and other harmful software?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are “No” then you should 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.

**Additional Risk Mitigations:**

**Section 4.0 Access to Records**

4.1	Is access to the system limited to only authorized individuals?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
4.2	Are requests for access approved and documented?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
4.3	Is access removed promptly upon the departure of an internal employee or upon notification of staff departures from external entities/users?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
4.4	Are individual accounts password protected?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
4.5	Does the system limit the number of failed login attempts?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are “No” then you should 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

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

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, 4. Automatically lock computers when left idle for a short period of time

**Additional Risk Mitigations:**

Section 5.0 Audit Trails		
5.1	Does the system have an audit trail to keep track of all records inserted along with any changes to records?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.2	Does the audit trail keep copies of deleted records?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.3	Does the audit trail ensure that the previously recorded information is still available (i.e. not obscured by the change)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.4	Does the system audit trail contain a time stamp which is applied automatically?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.5	Does the audit trail track changes in a consistent time zone?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.6	Does the audit trail keep track of the individual user who made the change?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.7	Does the system require entry of a reason for making the change?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.8	Is the audit trail protected from any individual modifying it or deleting it?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.9	Is it possible to discern invalid or altered records?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5.10	Is the audit trail available for review throughout the record's retention period?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<p><b>Possible Risk Mitigations and Corrective and Preventive Action (CAPA):</b> If any of the answers above are "No" then you should 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.</p>		
<p><b>Additional Risk Mitigations:</b></p>		

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

**Section 5.0 Audit Trails**

**Section 6.0 Operational Checks**

6.1	Is the computer system date and time synchronized to an international standard setting source?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.2	Does the system limit a user's ability to change date or time?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.3	Does the system include year, month, day, hour, minute, and time zone in time stamps on records?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.4	Does the system have checks to ensure steps are performed in the correct order if the sequence of system steps or events is important?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.5	Does the system contain prompts or other features to promote consistent use of terminology?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.6	Does the system contain checks to identify invalid values and alert the user?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.7	Does the system prevent default data entries or automatic duplication of data (unless programmed to do so)?	<input type="checkbox"/> Yes <input type="checkbox"/> No

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are "No" then you should 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 documentation.

**Additional Risk Mitigations:**

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: APP-A15-OPC-006.00

Section 7.0 Authority Checks		
7.1	Does the system ensure that only authorized individuals can use it, electronically sign records, alter records, or perform other operations as required?	<input type="checkbox"/> Yes <input type="checkbox"/> No
7.2	Does the system prompt for an individual's login account and password to prevent unauthorized users from accessing data?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p><b>Possible Risk Mitigations and Corrective and Preventive Action (CAPA):</b></p> <p>If any of the answers above are "No" then you should consider what mitigations of this risk are possible. Consider maintaining a cumulative record of authorized personnel, their titles, and a description of their access privilege. Consider maintaining a change log if the system does not utilize individual logins.</p>		
<p><b>Additional Risk Mitigations:</b></p>		

Section 8.0 Device Checks		
8.1	Does the system track which device or piece of equipment (e.g. vital sign, ECG, etc.) was used to capture the data? This applies only when more than one device is available for use.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<p><b>Possible Risk Mitigations and Corrective and Preventive Action (CAPA):</b></p> <p>If any of the answers above are "No" then you should consider what mitigations of this risk are possible. Consider recording this information in a comment on the record or some type of log.</p>		
<p><b>Additional Risk Mitigations:</b></p>		

Section 9.0 Training		
9.1	Do users of the system have sufficient education, training, and experience to perform the system tasks?	<input type="checkbox"/> Yes <input type="checkbox"/> No
9.2	Is this training documented?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

**Section 9.0 Training**

***Possible Risk Mitigations and Corrective and Preventive Action (CAPA):***

If any of the answers above are “No” then you should 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.

***Additional Risk Mitigations:***

**Section 10.0 Policies**

10.1	Is there a written policy for internal systems that ensures individuals are held fully accountable and responsible for actions initiated under their electronic signatures?	<input type="checkbox"/> Yes <input type="checkbox"/> No
------	---	--

***Possible Risk Mitigations and Corrective and Preventive Action (CAPA):***

If any of the answers above are “No” then you should 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.

***Additional Risk Mitigations:***

**Section 11.0 System Documentation**

11.1	Is the distribution of, access to, and the use of systems operation and maintenance documentation controlled?	<input type="checkbox"/> Yes <input type="checkbox"/> No
------	---	--

11.2	Are there procedures established to maintain an audit trail that documents version/change control sequenced development and modification of the system?	<input type="checkbox"/> Yes <input type="checkbox"/> No
------	---	--

***Possible Risk Mitigations and Corrective and Preventive Action (CAPA):***

If any of the answers above are “No” then you should 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.

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: APP-A15-OPC-006.00

**Section 11.0 System Documentation**

**Additional Risk Mitigations:**

**Section 12.0 Controls for Open Systems**

12.1	Are the data (at rest) encrypted on the storage device?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
12.2	Are the data (in motion) encrypted throughout the process of managing and/or transmitting the data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are "No" then you should consider what mitigations of this risk are possible.

**Additional Risk Mitigations:**

**Electronic Signature Requirements**

**Instructions:** If the system does NOT use electronic signatures, check the No box below, skip this entire section and proceed to the section requiring review signatures for this document

**System does not use electronic signatures**  No

**Section 13.0 Electronic Signature Components**

13.1	Does the signed electronic records contain the printed name of the signer?	<input type="checkbox"/> Yes <input type="checkbox"/> No
13.2	Does the signed electronic record contain the date and time of the signing (preferably with time zone)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
13.3	Does the signed electronic record contain the meaning of the signature that was applied (i.e. approval, review, etc.)?	<input type="checkbox"/> Yes <input type="checkbox"/> No

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

**Section 13.0 Electronic Signature Components**

If any of the answers above are “No” then you should consider what mitigations of this risk are possible.

**Additional Risk Mitigations:**

**Section 14.0 Signature as Electronic Record**

14.1	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 (i.e. on an electronic display screen or on a report)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
------	---	--

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are “No” then you should consider what mitigations of this risk are possible.

**Additional Risk Mitigations:**

**Section 15.0 Electronic Signature Linking**

15.1	Are the electronic signatures linked to its respective electronic record to ensure that the signature cannot be removed, copied, cut and pasted, or transferred by ordinary means in order to falsify an alternate electronic record?	<input type="checkbox"/> Yes <input type="checkbox"/> No
15.2	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?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are “No” then you should consider what mitigations of this risk are possible.

**Additional Risk Mitigations:**

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

<b>Section 16.0 Electronic Signature Uniqueness</b>		
16.1	Are electronic signatures unique to an individual?	<input type="checkbox"/> Yes <input type="checkbox"/> No
16.2	Are you ensuring that an electronic signature is never reused by or reassigned to anyone else?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Possible Risk Mitigations and Corrective and Preventive Action (CAPA):</b>  If any of the answers above are "No" then you should 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.		
<b>Additional Risk Mitigations:</b>		

<b>Section 17.0 Identity Verification</b>		
17.1	Are you verifying the identity of the individual before providing them the ability to sign electronically?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Possible Risk Mitigations and Corrective and Preventive Action (CAPA):</b>  If any of the answers above are "No" then you should consider what mitigations of this risk are possible. Establish a process for verifying identity and include this process in the account management policy/procedure.		
<b>Additional Risk Mitigations:</b>		

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

**Section 18.0 Electronic Signature Certification (for internal staff users only)**

11.100 (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5601 Fishers Lane, Rockville, Maryland (MD) 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

18.1	Have you submitted plans in writing to use electronic signature to the FDA, EMA or any other regulatory authority?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
------	--	---

**Section 19.0 Electronic Signature Components**

19.1	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)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
19.2	Does the system prompt for a re-entry of the password or pin upon each application of the electronic signature?	<input type="checkbox"/> Yes <input type="checkbox"/> No
19.3	Does the system prompt for both components when the signing is not performed during a single, continuous period of controlled system access?	<input type="checkbox"/> Yes <input type="checkbox"/> No
19.4	Are electronic signatures only used by their genuine owners (applicable to sites)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
19.5	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?	<input type="checkbox"/> Yes <input type="checkbox"/> No

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are "No" then you should 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.

**Additional Risk Mitigations:**

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

**Section 19.0 Electronic Signature Components**

**Section 20.0 Biometric Electronic Signatures**

20.1	Can it be shown that biometric electronic signatures can only be used by their genuine owners?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
------	--	---

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are “No” then you should consider what mitigations of this risk are possible. Ensure any biometric that may be used (i.e. fingerprints, retinal scans, etc.) are truly unique to the individual.

**Additional Risk Mitigations:**

**Section 21.0 Electronic Signature Management**

21.1	Are controls in place to maintain the uniqueness of the user ID and password so that no individual can have the same combination?	<input type="checkbox"/> Yes <input type="checkbox"/> No
21.2	Are passwords required to be reset as some set periodic interval?	<input type="checkbox"/> Yes <input type="checkbox"/> No
21.3	Are processes in place to deactivate lost, stolen, missing or otherwise compromised tokens, cards, that are used for electronic signature purposes?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
21.4	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?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
21.5	Does the system have safeguards to prevent unauthorized use of passwords and/or identification codes?	<input type="checkbox"/> Yes <input type="checkbox"/> No

**Possible Risk Mitigations and Corrective and Preventive Action (CAPA):**

If any of the answers above are “No” then you should consider what mitigations of this risk are possible. Consider an account management policy or procedure that applies specific rules for assigning user IDs, requires password resets if they cannot be forced by the system, assures users log out when leaving their workstation unattended. Provide a means for personnel to report lost, stolen or missing tokens or devices and consider how to manage these items including the revoking of the token’s validity. Include controls to assure the person is

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

**Section 21.0 Electronic Signature Management**

identified before providing the user with a password reset or temporary device. A process for collecting the tokens, devices, etc. from personnel when they depart from employment. Consider also including periodic review of all user IDs, tokens, etc. to ensure they are still needed, still have appropriate access and still function properly. Consider including in a policy the requirement for reporting immediately to management any unauthorized use of user IDs, passwords, tokens, devices, etc.

***Additional Risk Mitigations:***

EFFECTIVE

Appendix B:  
**Electronic Information System Evaluation Checklist**

Effective Date: 08/21/20

Document No.: **APP-A15-OPC-006.00**

**Review Acknowledgement**

**Section 22.0 Assessor Acknowledgement**

*By signing this document, you indicate that the information contained within this document is accurate and complete to the best of your knowledge.*

<p>&lt;Name&gt; &lt;Title&gt;</p>	<p>Signature:</p>	<p>Date:</p>
---------------------------------------	-------------------	--------------

**Section 23.0 CRS Leader or DMC Director (as applicable)**

*By signing this document, you indicate that you have reviewed and approve the information contained within this document.*

<p>&lt;Name&gt; &lt;Title&gt;</p>	<p>Signature:</p>	<p>Date:</p>
---------------------------------------	-------------------	--------------

**REVISION HISTORY**

1. APP-A15-OPC-006.00 is the original version of this Appendix.