BRICS Report on 21 CFR Part 11 Compliance

Document Information

Document Owners: Matthew McAuliffe, Yang Fann, and Dominic Nathan

Organizations: NINDS DIR ITBP, CIT OIR ISL BIRSS, CNRM

Approval / Distribution Process

The SOP approval/distribution process is as follows:

1. The SOP author sends the SOP SharePoint link to their peers/subject matter experts (SMEs) for review.
2. After editing, the SOP author decides whether the SOP is ready for approval. If the SOP is ready, the author adds the SOP to the ITBP Manager meeting agenda.
3. At the ITBP Managers meeting or via email, NINDS Management formally approves/disapproves the SOP.
4. The SOP Author sends the SOP link to all people on the Distribution List.

NINDS Approval

This Standard Report is approved for distribution and implementation as of the Director ITBP approval date listed below. NINDS ITBP management is authorized to conduct periodic audits to ensure compliance with this procedure. Requests for corrections or changes to any part of this procedure must be submitted to the Document Owner to review. Exceptions to any procedure must be approved by the ITBP Management and documented.

Approved By:

Name	Title	Organization	Approval Date
Yang Fann	IT Director	NINDS DIR ITBP	04/25/19
Matthew McAuliffe	BIRSS Chief	CIT OIR ISL BIRSS	04/25/19
Dominic Nathan	Informatics Core Director	CNRM	04/25/19

Name	Title	Organization	Approval Date
Mark Edwards	IT Manager	NINDS DIR ITBP	04/25/19
Willy Calderon	ISSO	NINDS DIR ITBP	04/25/19

Peer Reviewers

This Standard Report was reviewed by the peers (i.e., subject matter experts) listed below. The procedure will be reviewed by the peer reviewers at least annually.

Reviewed By:

Name	Title	Organization	Date
Tsega Gabremichael	Team Lead	CIT OIR ISL BIRSS	03/27/19
Leonie Misquitta	Sr Scientific Advisor	CIT OIR ISL BIRSS	03/27/19
Dominic Nathan	Informatics Core Director	CNRM	03/27/19

Distribution List

This Standard Report impacts the individuals on this Distribution List. The report author should notify everyone on this list about changes to this SOP *within one week* of NINDS approval.

Distributed To:

Name / Department / Group / Team
Yang Fann
Matthew McAuliffe
Dominic Nathan
Willy Calderon

1. Introduction

1.1 Overview

This document summarizes the self-evaluation and assessments against the 21 CFR Part 11 Compliance for the BRICS and its associated systems such as CiSTAR, CASA, and ProFoRMS at NINDS, CIT and CNRM. The intended audience for this report includes the groups/individuals listed below:

- NINDS DIR Clinical Informatics Development Team
- CIT OIR ISL BIRSS Development Team
- Business stakeholders and partners

1.2 Purpose

This Standard Report serves two purposes:

a) It serves as a declaration of the remediation results after reviewing the Proposed Solutions for Corrective Actions from the Part 11 assessor/advisor on March 11, 2019.

b) It provides instructions of the package for assessors to use. This can help provide reasonable assurance that a consistent level of reporting is present.

1.3 Scope

This Standard Report provides a comprehensive summary of remediation actions, testing activities performed and information collected during the self-evaluation against the 21 CFR Part 11 Compliance. The information package covers enough details to verify the requirements for full compliance and recertification.

1.4 Results of the Part 11 Evaluation in March

The following system summary report is a helpful representation from the Part 11 advisor's comments on Monday, March 11, 2019:

BRICS / CiSTAR / CASA Clinical Trial Software

System Description and Specifications

Field	Value
Owner	Dominic Nathan
Trained	☑
Backup Owner	
Trained	☐
Site	
Department	
Record Type	
Priority	

General description

What kind of records are input or exported?

Where and how is this data used?

Field	Value	Field	Value
Manufacturer	NINDS and CIT	Mfg Contact	
Product Name		Contact Emai	
Software Ver.	3.6	Contact Number	
Database		Date Installed	
Database Ver.		Date Validated	
		Physical Location	
Equip. Model #		Network Location	
OS Ver.		System URL	

Results of the Evaluation

Section	Requirement	Score
Subpart B : Electronic Records	**Electronic Records Score:**	**82.5 %**
11.10	Controls for Closed Systems	84.6%
11.30	Controls for Open Systems	100.0%
11.50	Signature Manifestations	67.5%
11.70	Signature and Record Linking	100.0%
Subpart C : Electronic Signatures	**Electronic Signatures Score:**	**86.7 %**
11.100	Electronic Signature General Requirements	50.0%
11.200	Controls for Electronic Signatures	100.0%
11.300	Controls of Identification Codes and Passwords	100.0%

BRICS / CiSTAR / CASA Clinical Trial Software 84.4%

1.5 Proposed Solutions for Corrective Actions

The following findings identified by the assessor for the first time:

BRICS / CiSTAR / CASA Clinical Trial Software

Solution	Score	Sect / Sys	Cost	Approved?
From 11.10(e), Audit Trails				
Add audit trail functionality to the system	**100%**	**Section**	**$0**	**Yes**

Task Description	*Time*	*Cost*	*Target*	*Status*
See if AT can be turned on for Data Entry	0	$0	4/27/2019	Pending
See if first entries are captured after lock	0	$0	4/27/2019	Pending
Re-test to verify all data is traceable to a single person.	0	$0	4/27/2019	Pending

Summary for BRICS / CiSTAR / CASA Clinical Trial Software

Total time (days): 0
Total estimated cost: $0

Total est. time (days): 0
Total est. cost: $0

1.6 System Evaluation Result Details

At each subpart requirement, under the Part 11 regulation, there are observation and score columns in which to designate the result.

BRICS / CiSTAR / CASA Clinical Trial Software 84.4%

Subpart B. Electronic Records 82%

Section 11.10 Controls for Closed Systems 85%

Regulation	*Observation*	*Score*
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	System has been validated. The core system and all elements for each study is validated.	100%
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	All raw data can be printed or exported, but some meta data cannot be exported. Signatures could not be exported for signed records.	90%
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Records are automatically archived on a secure server for the full record retention period as defined by our SOP. Currently all data is kept online permanently.	100%
(d) Limiting system access to authorized individuals.	System has multi-level security that restricts access to authorized individuals. Entry is restricted to named users with login ID's and passwords.	100%
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	The system records the date, time, and name of the person who created the initial record. Additionally, there are no audit trail records genereated for any changes until the first lock is implemented. After first lock, data entry users are locked out and all changes to existing data is properly tracked in the audit trail.	25%
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Steps cannot be executed in the wrong order.	100%
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	The system checks authority rights. There are multiple XXX	100%

Regulation	*Observation*	*Score*
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	This application has been validated to verify only authorized users can gain access to this system. The IT group utilizes firewalls and constantly monitors the system to prevent unauthorized access, and all IP addresses are recorded. NIST 800-53 ?xxx meets these Meets Federal inst stuff xxx	100%
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Users are trained on proper use of the system before access is granted. Each user is given orientation training for their job or role for how to create studies, enter data, etc.	100%
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	We do not have any written policies for electronic records or signatures.	0%
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	This is handled by document control.	100%
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	This is handled by change control within document control.	100%

Section 11.30 Controls for Open Systems 100%

Regulation	*Observation*	*Score*
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	This is an open system that uses https and database encryption to protect the integrity of the data.	100%

Section 11.50 Signature Manifestations 67%

Regulation	Observation	Score
(1) The printed name of the signer;	A valid login ID is required for login and is linked to that persons full printed name (first and last name) within the software.	95%
(2) The date and time when the signature was executed;	The local date and time is stored with the record.	100%
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The meaning of the signature is available at the time of signing but is not saved with the signature.	0%
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	The signature information is saved separately from the record and can be retrieved upon request minus the meaning.	75%

Section 11.70 Signature and Record Linking 100%

Regulation	Observation	Score
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	The user cannot alter an electronic signature.	100%

Subpart C. Electronic Signatures 87%

Section 11.100 Electronic Signature General Requirements 50%

Regulation	Observation	Score
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Electronic signatures are unique to one individual.	100%
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Verifying the identity of the individual is captured in the SOP on adding new users. The process to gain access to the system starts with a request from the investigater and confirmation of training.	100%
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	This letter has not been submitted by our company. (A sample letter is available at http://www.ofnisystems.com/information/resources/sample-letters-of-non-repudiation-agreement/)	0%

Regulation	Observation	Score
(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.	xxxx add to initial training	0%

Section 11.200 Controls for Electronic Signatures 100%

Regulation	Observation	Score
(1) Employ at least two distinct identification components such as an identification code and password.	A username and password is required to apply an electronic signature.	100%
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by the individual.		100%
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	The system will automatically lock down after a short period of time, and we have to re-enter our password to unlock the application.	100%
(2) Be used only by their genuine owners;	An SOP (nist 8xxx)requires that passwords are only known to their owners.	100%
(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	There is a separation of responsibilities to ensure that those who are responsible for the data and records do not have these rights. The clinical trial units and the IT departments are kept completely separate.	100%
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A - Biometrics are not used or available for signatures on this system.	100%

Section 11.300 Controls of Identification Codes and Passwords 100%

Regulation	Observation	Score
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Each individial has their own unique login ID and password that is only known by that person.	100%
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The software does have controls to enforce password complexity and requirements for periodically changing passwords.	100%

Regulation	Observation	Score
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	N/A - Devices cannot be used to gain access or interact with this software.	100%
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	The software has an event log that records actions and events like logins, logouts, and changes to individual user security settings. These logs can be extracted from the DBA or from the web server log files.	100%
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	N/A - Devices cannot be used to gain access or interact with this software.	100%

2. Corrective Actions

This section summarizes the corrective actions taken to resolve these findings explicitly stated in Section 1, where each finding was first reported, the conditions observed with evaluation scores. The technical team has addressed these issues in E-signature, audit log, and documentation three important areas. The status and details for each subpart requirement are listed in the table below. The requirements with Work In Progress (WIP) status will be fulfilled upon software release.

Req	Subpart	Findings	Score	Status	Action
	11.10	***Controls for Closed Systems***	***85%***		
1	(b)	All raw data can be printed or exported, but some meta data cannot be exported.	90%	WIP	Addressed by the technical team
2	(b)	Signatures could not be exported for signed records.	90%	WIP	Addressed by the technical team
3	(e)	System records the date, time, and name of the person who created the initial record. There are no audit trail records generated for any changes until the first lock is implemented.	25%	WIP	Addressed by the technical team
4	(j)	Written policy hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	0%	Completed	All associated documents are available including E-Signature written policy (in Sec.3)
	11.50	***Signature Manifestations***	***67%***		

5	(3)	The meaning (such as review, approval, responsibility, or authorship) of the signature is available at the time of signing but is not saved with the signature.	0%	WIP	Addressed by the technical team
	11.100	***E-Signature General Requirements***	***50%***		
6	(1)	The certification letter has not been submitted by the company.	0%	Completed	
7	(2)	Persons using e-signatures shall, upon agency request, provide additional certification or testimony that a specific e-signature is the legally binding equivalent of the signer's handwritten signature.	0%	Completed	All associated documents are available including E-Signature written policy (in Sec.3)
		System Evaluation Results	**84.40%**		

3. Documentation

The list of the following documents is included in the package for review and recertification:

Reference Number	Document Name	Document Purpose
BRICS-Doc-1	BRICS_Report_Compliance	Compliance Report
BRICS-Doc-2	BRICS_E_Signature_Security_Policy	Electronic Signature Security Policy
BRICS-Doc-3	BRICS_System_Access_Logs_SOP	System Access Logs
BRICS-Doc-4	BRICS_Software_Development_Process_SOP	Software Development Process
BRICS-Doc-5	BRICS_SRS_SOP	System Requirements Specification

Reference Number	Document Name	Document Purpose
BRICS-Doc-6	BRICS_Design_Document_SOP	System Design Document
BRICS-Doc-7	BRICS_MTP	Master Test Plan
BRICS-Doc-8	BRICS_User_Guidelines	User Guides

4. Records management

All data and/or records generated during this procedure are stored in the NINDS SharePoint-based Document Library.

5. Review/Revision History

Date	Author/Reviewer	Description of Change
03/19/2019	Gladys Wang	Document Creation