Ofni Systems

Ofni Systems Inc.
808 Salem Woods Dr, Suite 103
Raleigh, NC 27615
Phone: (919) 844-2494
Fax: (919) 869-1990
Info@OfniSystems.com

May 15, 2019

Center for Neuroscience & Regenerative Medicine (CNRM)
Uniformed Services University of the Health Sciences
Henry M. Jackson Foundation Contractor
Dominic Nathan
12725 Twinbrook Parkway
Rockville, MD 20852

Dr. Nathan:

This letter is to acknowledge that the BRICS software has successfully undergone a gap analysis for 21 CFR Part 11, Electronic Records, Electronic Signatures. We are pleased to report that all issues have been addressed, and the software has met all the technical and procedural requirements of the regulation.

Sincerely,

Tyson Mew

Tyson Mew
President

System Evaluation Results

BRICS Clinical Trial Software 100.0%

Subpart B. Electronic Records 100%

Section 11.10 Controls for Closed Systems 100%

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, including meta data and signatures for signed records.	100%
(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 and also for any changes after the record is created. After first lock, data entry users are prevented from making edits, but administrators can edit locked records and all changes to existing data is properly tracked in the audit trail.	100%
(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 for multiple operations within the software.	100%

Section 11.10 Controls for Closed Systems 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. All requirements for NIST 800-53 are also met.	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, and all other regulated tasks.	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 have written policies for electronic records and signatures.	100%
(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 100%

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.	100%

Section 11.50 Signature Manifestations 100%

Regulation	*Observation*	*Score*
(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 and is saved with the signature.	100%
(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 or printed.	100%

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 100%

Section 11.100 Electronic Signature General Requirements 100%

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 been submitted by our organization.	100%
(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.	This is handled by our HR department. All new employees sign a statement to confirm they understand that electronic signatures are the legally binding equivalent of traditional handwritten signatures.	100%

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.	The system will automatically log us out of the software after a short period of time, and we have to re-enter our password to log back into the application.	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 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%
(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%

Section 11.300 Controls of Identification Codes and Passwords 100%

Regulation	*Observation*	*Score*
(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%