ICH GCP AND FDA 21 CFR PART 11 COMPLIANCE STATEMENTS

April 2017

Dynacare is one of Canada’s largest providers of laboratory services and solutions to Patients, Healthcare Professionals and Corporate Clients with the collection and transportation of specimens, and accurate testing. In addition to diagnostic services, Dynacare participates in the Clinical Trial industry which requires the Laboratory Information System (LIS) used in regulated activities be validated and 21 CFR Part 11 compliant.

The Dynacare LIS system is validated and 21 CFR Part 11 compliant. The LIS Validation generated system design and testing documentation to meet ICH GCP 5.5.3, sections a - g and 21 CFR Part 11, section 11.10. Based on a detailed Part 11 assessment of the LIS system, it is considered a “Closed System”.

ICH GCP 5.5.3, sections a-g requirements

When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

(a) Ensure and document that the electronic data processing system(s) conforms to the sponsor’s established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e. validation).

(b) Maintains SOPs for using these systems.

(c) Ensure that the systems are designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e. maintain an audit trail, data trail, edit trail).

(d) Maintain a security system that prevents unauthorized access to the data.

(e) Maintain a list of the individuals who are authorized to make data changes.

(f) Maintain adequate backup of the data.

(g) Safeguard the blinding, if any (e.g. maintain the blinding during data entry and processing).
21 CFR Part 11 Requirements

The regulation set forth the criteria, under which the FDA considers electronic records, electronic signatures, and handwritten signatures that are executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

Components of 21 CFR PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES:

Subpart A — General Provisions

11.1 Scope.
11.2 Implementation.
11.3 Definitions.

Subpart B — Electronic Records

11.10 Controls for closed systems.
11.30 Controls for open systems.
11.50 Signature manifestations.
11.70 Signature/record linking.

Subpart C—Electronic Signatures

11.100 General requirements.
11.200 Electronic signature components and controls.
11.300 Controls for identification codes/passwords.

Dynacare Compliance to Regulations:
Subpart A — General Provisions

11.1 Scope

- The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

- This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any record requirements set forth in agency regulations. Additionally, this part applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.
• Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically accepted by regulation(s) effective on or after August 20, 1997.

• Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2 unless, paper records are specifically required.

• Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

Compliance: Dynacare (LIS) system relies on electronic records for regulated activities. Electronic records are created, modified, maintained, archived, retrieved, or transmitted in support of regulated activities for Clinical Trials. Dynacare uses Electronic Signatures where appropriate and required.

11.2 Implementation

• For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

• For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:
  ➢ The requirements of this part are met; and
  ➢ The document or parts of a document to be submitted have been identified in public docket No. 92S- 0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, and branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.
Compliance: Dynacare does not submit electronic records directly to the FDA. Data generated by the laboratory is transmitted to the Study Sponsor which submits the appropriate information to the FDA for drug submission purposes. Dynacare electronic records not submitted to the FDA are generated by the Laboratory Information System which is compliant to the 21 CFR Part 11 regulations.

11.3 Definitions

- The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.
- The following definitions of terms also apply to this part:
  - Agency means the Food and Drug Administration.
  - Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
  - Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
  - Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
  - Electronic record means any combination of text, graphics, data, and audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
  - Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
  - Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate writing in a permanent form. The act of signing with a writing or marking instruments such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
  - Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Compliance: Dynacare recognizes and uses the terms and definitions of regulation.
Subpart B — Electronic Records

11.10 Controls for Closed Systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

- Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

**Compliance:** The Laboratory Information System is validated. A comprehensive system retrospective validation approach was used to ensure data accuracy, reliability and integrity.

- A Validation package was created and is maintained based on an established Software Development Methodology and Change Control SOPs.
- The validation approach was based on GAMP 5 — “V-Model” which includes deliverables such as a Validation Plan, Risk Assessment, Functional Requirements, Technical Requirements, Test Documentation, Traceability Matrix and a Validation Summary.
- ITSS and Operations were involved in the system retrospective validation and QA audited the deliverables for compliance to the Validation Plan, Functional Requirements, Regulations, Polices and SOPs.

The compliance to 11.10(a) can be applied to ICH GCP 5.5.3, section a:

(a) Ensure and document that the electronic data processing system(s) conforms to the sponsor’s established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e. validation).

- 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.

**Compliance:** Dynacare is able to create copies of records for Regulatory and Client Audits.
• Protection of records to enable their accurate and ready retrieval throughout the records retention period.

**Compliance:** Dynacare has procedures to backup and restore electronic records throughout the retention period.

**The compliance to 11.10(c) can be applied to ICH GCP 5.5.3, section f:**

(f) Maintain adequate backup of the data.

• Limiting system access to authorized individuals.

**Compliance:** Dynacare has procedures to control access to the physical location, server room, Network and LIS.

**Security**

➢ The LIS has multiple levels of security to ensure that data is protected.
➢ The LIS has role-based security based on job function.
➢ Physical access to the site and data center is restricted to authorized personnel only. Access is monitored 24/7.
➢ Remote access is controlled by implementing a Virtual Private Network (VPN) security model and firewalls.

**The compliance to 11.10(d) can be applied to ICH GCP 5.5.3, sections d and e:**

(d) Maintain a security system that prevents unauthorized access to the data
(e) Maintain a list of the individuals who are authorized to make data changes.

• 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.

**Compliance:** Dynacare LIS has an audit trail which records all changes to data.

**Audit Trail**

• The audit trail tracks Who, What, Where, When and Why a change was made to data.
• The audit trail is system generated and cannot be modified by users.
• Audit trails are available for Internal/External (regulatory and client) audits
The compliance to 11.10(e) can be applied to ICH GCP 5.5.3, section c:

(c) Ensure that the systems are designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e. maintain an audit trail, data trail, edit trail).

- Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

**Compliance:** Dynacare LIS has defined workflows which allow the sequencing of regulatory activities.

- 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.

**Compliance:** Dynacare LIS has defined Authority Checks through its role security.

- Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

**Compliance:** Devices such as Analyzers are installed and configured in the Dynacare LIS. Devices must be configured to use a specific communication protocol and must be uniquely identified prior to use.

- Determination that persons who develop, maintain, or use electronic record/electronic signature systems has the education, training, and experience to perform their assigned tasks.

**Compliance:** Dynacare utilizes the Human Resources Department to ensure that qualified employees are hired for all positions. LIS training is a controlled and documented process which ensures that users are fully trained to perform their job function.

- 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.

**Compliance:** Electronic Signature Testimonial is completed and signed by each Dynacare employee as part of the onboarding process. The signed document verifies the identity of a person who will be using an electronic signature (user ID, login password and e-signature password) at Dynacare. The testimonial also pertains to the employee being aware of the following:
• The Electronic Signature is unique to each employee and shall not be reused or assigned to anyone else
• The employee is held responsible for all actions initiated under their electronic signature
• The electronic signature is the legal equivalent of traditional handwritten signature
• The electronic signature shall only be used for those assigned tasks that the employee has the authority, education, training and experience to perform

• Use of appropriate controls over systems documentation including:
  ➢ Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
  ➢ Revision and change control procedures to maintain an audit trail that documents time-sequenced, development and modification of systems documentation.

**Compliance:** Dynacare has a defined Document Control process which covers the creation, revision and distribution of SOPs and other essential documentation.

The compliance to 11.10(k) can be applied to ICH GCP 5.5.3, section b:
(b) Maintains SOPs for using these systems.

The compliance to ICH GCP 5.5.3, section G:
• Safeguard the blinding, if any (e.g. maintain the blinding during data entry and processing).

**Compliance:** Trial Subject ID information is an Alpha-Numeric identifier provided by either the Sponsor or Investigator which cannot be traced back to an individual by Dynacare staff members.
Sec. 11.30 Controls for Open Systems

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.

Compliance: Dynacare LIS is considered a closed system due to security controls and architecture implemented to allow only authorized individual to access the LIS system or its data.

Sec. 11.50 Signature Manifestations

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:
   1. The printed name of the signer;
   2. The date and time when the signature was executed; and
   3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(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).

Compliance: Dynacare uses Electronic Signatures where appropriate and required.

All reviewed and approved electronic data contains the following information:

- The actual name of the user along with the username
- The date and time
- The user is also prompted when appropriate to obtain the reason for their operational action

Human readable reports are setup to display the data logged to the secure relational database and are available to be viewed by regulatory agencies.
Sec. 11.70 Signature/Record Linking

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.

Compliance: Dynacare does not use hybrid Electronic Signatures; this section is not applicable.

Subpart C — Electronic Signatures

11.100 General Requirements.

- Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
- 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.

Compliance: Dynacare security ensures that security identifier is unique between all users. Electronic Signature Testimonial is completed and signed by each employee as part of the onboarding process. The signed document verifies the identity of a person who will be using an electronic signature (user ID, login password and e-signature password) at Dynacare.

11.200 Electronic Signature Components and Controls

- Electronic signatures that are not based upon biometrics shall:
  Employ at least two, distinct identification components such as an identification code and password.
    - When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.
    - 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.
• Be used only by their genuine owners; and
• 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.
• Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners

**Compliance:** Dynacare security is used to provide a username and password for each user. For a user to log into the system, they will be required to use both their username and password to gain access. Subsequent system data entries will require only the password entered by the user (this is the signature component that is known only to, and usable by, the user). System in which electronic signature is used are setup to logout a user after a time with no user activity and procedures should be used to ensure that users do not leave the terminal unattended during their session.

**11.300 Controls for Identification Codes/Passwords.**

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

• Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
• Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
• Following loss management procedures to electronically de-authorize 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.
• 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.
• 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.

**Compliance:** Dynacare ensures that all user names are unique. Passwords are validated to confirm they have a minimum length and are revised every three month. Dynacare uses transaction safeguards to prevent unauthorized use of passwords. Security certificates are periodically reviewed and revised by the ITSS security team. Dynacare does not employ the use of codes generated by tokens or devices.
Conclusion:
The LIS system based on all documented activities, regulatory and client expectations is considered 21 CFR Part 11 compliant.

Sincerely,

[Signature]

Dennis Haikalis
Director, Corporate Quality Programs
Dynacare