U.S. FDA CFR 21 Part 11 Compliance Assessment

Leading2Lean cloudDispatch SaaS Solution

Contents

Disclaimer

These materials are subject to change without notice. Leading2Lean's compliance analysis with respect to Leading2Lean's software performance based on FDA Title 21 CFR Part 11: (i) in no way expresses the recognition, consent or certification of Leading2Lean software by the U.S. Food and Drug Administration; and (ii) applies to certain of the Leading2Lean's cloudDispatch SaaS solution live production version being delivered in November 2018 only as stated herein. The customer is solely responsible for compliance with all applicable regulations, and Leading2Lean and its affiliate companies or subsidiaries have no liability or responsibility in this regard. These materials are provided by Leading2Lean for informational purposes only, without representation or warranty of any kind, and Leading2Lean shall not be liable for any errors or omissions with respect to the materials. The only warranties for Leading2Lean products or services are those set forth in the expressed warranty statements accompanying Leading2Lean subscription services, if any. Nothing herein should be construed as constituting an additional warranty.

Executive Summary

U.S. Food and Drug Administration

The FDA monitors the manufacture, import, transport, storage, and sale of products including:

- Food for human and animal consumption
- Pharmaceuticals consisting of ethical, generic, and over-the-counter drugs for human use as well as medicines for animals
- Biological and related products including blood, vaccines and biological therapeutics
- Medical devices
- Radiation-emitting devices such as microwaves
- Cosmetics

Compliance with FDA regulations is a market requirement. In addition, products require FDA approval before they can be marketed or sold in the United States. Noncompliance with any of the laws enforced by the FDA can be very costly in the form of recalls and legal sanctions, such as import detentions. When warranted, FDA seeks criminal penalties, including prison sentences, against manufacturers and distributors. Due to the critical nature to consumers of products controlled by FDA regulations, manufacturers of these products require both comprehensive record keeping of certain activities and a quality production system to assure consistent quality and safety of these products. Electronic record systems, while authorized as a method of maintaining the records required by each part of the FDA regulations, must also meet requirements to assure proper record retention and access is available when needed. Clarification to electronic records and electronic signatures is now contained in Part 11 of CFR 21 to provide clear guidance to medical manufacturers and to allow for innovation and modernization.

Based on the interpretation of FDA Title 21 CFR Part 11 rule of the U.S. Food and Drug Administration and the functions and features discussed within this document, Leading2Lean believes the cloudDispatch SaaS solution version currently being deployed in November 2018 as a managed service technically complies with the intent and requirements of the Part 11 rule.

21 CFR Part 11 Electronic Records, Electronic Signatures; File Rule

FDA regulation 21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule (Part 11) was the result of a six-year effort by FDA (with input from the industry) to supply all FDA-regulated companies with requirements on how to maintain paperless (electronic) record systems while still complying with good clinical, laboratory, and manufacturing practices, such as:

- GMP; 21 CFR 110 (food), 210 (drugs in general, includes GMP for biologics), 211 (finished pharmaceuticals), 820 (medical devices)
- Good laboratory practice (GLP) 58
- Good clinical practice (GCP) 50, 54, 56

The regulation also details very specific requirements for electronic and digital signatures, because FDA considers these signatures to be legal and binding.

Since its publication more than nine years ago, this regulation has been subject to evolving interpretations both by the FDA and industry.

In February 2003 FDA withdrew all Part 11 guidelines and the Compliance Policy Guide. The reasons for the withdrawal are discussed in the FDA document from August 2003, "Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application " as follows;" ... concerns have been raised that some interpretations of the part 11 requirements would (1) unnecessarily restrict the use of electronic technology in a manner that is inconsistent with FDA's stated intent in issuing the rule, (2) significantly increase the costs of compliance to an extent that was not contemplated at the time the rule was drafted, and (3) discourage innovation and technological advances without providing a significant public health benefit. These concerns have been raised particularly in the areas of part 11 requirements for validation, audit trails, record retention, record copying, and legacy systems."

In April of 2012, the FDA published an updated CFR 21, Part 11 to reflect the guidance outlined above. This added Subpart C to the existing Part 11 outlining electronic signature components and controls as well as controls for identification and passwords.

CFR21 Part 820 - Quality System Requirements

CFR 21 Part 820 defines responsibilities of manufacturers to define and implement quality production systems, maintain records of preventative maintenance (PM) and validate software used as part of the quality system. This includes maintenance schedules for PM, but also includes, in paragraph (i), a reference to software systems used. This section outlines the

manufacturer of medical devices to meet requirements in several areas and includes specific areas where Leading2Lean's cloudDispatch solution could be used. The following sub paragraphs are excerpts from Part 820:

(g)Equipment. Each manufacturer shall ensure that all equipment used in the manufacturing process meets specified requirements and is appropriately designed, constructed, placed, and installed to facilitate maintenance, adjustment, cleaning, and use.

(l)Maintenance schedule. Each manufacturer shall establish and maintain schedules for the adjustment, cleaning, and other maintenance of equipment to ensure that manufacturing specifications are met. Maintenance activities, including the date and individual(s) performing the maintenance activities, shall be documented.

(2)Inspection. Each manufacturer shall conduct periodic inspections in accordance with established procedures to ensure adherence to applicable equipment maintenance schedules. The inspections, including the date and individual(s) conducting the inspections, shall be documented.

(3)Adjustment. Each manufacturer shall ensure that any inherent limitations or allowable tolerances are visibly posted on or near equipment requiring periodic adjustments or are readily available to personnel performing these adjustments.

(h)Manufacturing material. Where a manufacturing material could reasonably be expected to have an adverse effect on product quality, the manufacturer shall establish and maintain procedures for the use and removal of such manufacturing material to ensure that it is removed or limited to an amount that does not adversely affect the device's quality. The removal or reduction of such manufacturing material shall be documented.

(i)Automated processes. When computers or automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer software for its intended use according to an established protocol. All software changes shall be validated before approval and issuance. These validation activities and results shall be documented.

CFR21 Part 820, Subpart M – Records

Additionally, Subpart M of Part 820 also outlines specific records requirements that pertain to those activities above:

Subpart M-Records

Sec. 820.180 General requirements.

All records required by this part shall be maintained at the manufacturing establishment or other location that is reasonably accessible to responsible officials of the manufacturer and to employees of FDA designated to perform inspections. Such records, including those not stored at the inspected establishment, shall be made readily available for review and copying by FDA employee(s). Such records shall be legible and shall be stored to minimize deterioration and to prevent loss. Those records stored in automated data processing systems shall be backed up.

(a)Confidentiality. Records deemed confidential by the manufacturer may be marked to aid FDA in determining whether information may be disclosed under the public information regulation in part 20 of this chapter.

(b)Record retention period. All records required by this part shall be retained for a period of time equivalent to the design and expected life of the device, but in no case less than 2 years from the date of release for commercial distribution by the manufacturer.

(c)Exceptions. This section does not apply to the reports required by 820.20(c) Management review, 820.22 Quality audits, and supplier audit reports used to meet the requirements of 820.S0(a) Evaluation of suppliers, contractors, and consultants, but does apply to procedures established under these provisions. Upon request of a designated employee of FDA, an employee in management with executive responsibility shall certify in writing that the management reviews and quality audits required under this part, and supplier audits where applicable, have been performed and documented. the dates on which they were performed. and that any required corrective action has been undertaken.

FDA Title 21 CFR Part 11 Assessment of cloudDispatch

Security and Confidentiality

Dispatch executes authority checks on login to the subscribed service. All Users require a valid username and password for login and are required to access a URL specifically designated for the customer. User accounts for granting access are configured, and specific areas of the application are authorized access, by the customer's designated cloudDispatch administrator(s).

The cloudDispatch service can be configured to force a change in passwords periodically. Previously used passwords are not allowed. Passwords must include combinations of alphanumeric characters and cannot contain the username. Usernames and passwords can be

inactivated for use by the customer's cloudDispatch administrator when employees leave the company or no longer require access.

An electronic record of all failed login attempts is maintained in the cloudDispatch access. Changes to user records or access permissions are also captured in electronic records.

cloudDispatch is configured to use SSL/TLS (HTTPS) to assure usernames, passwords, data entry and queries to any electronic records are secure from electronic monitoring methods. Data entries performed by users that are authorized to create events, captures the origin machine IP as part of the electronic record. The customer URL for access to cloudDispatch records can also be restricted to allow only specific private IP domains access. Such restriction limits use to only IP networks within the customer's locations and excludes public access from public cell services used by smart phones and tablet devices (i.e. iPad, Android, etc).

AICPA SOC 2 Compliance

Maintaining a highly available, secure, enterprise grade solution is a critical characteristic of the Leading2Lean cloudDispatch solution. To achieve our high standards of quality, Leading2Lean has invested heavily in designing and operating our service to adhere to the American Institute of Certified Public Accountants (AICPA) SOC 2 SaaS industry standard.

SOC 2 compliance evaluates that Leading2Lean controls meet the criteria for security, availability, and confidentiality in the AICPA TSP section 100, Trust Services. SOC 2 is the industry standard for online SaaS solutions. SOC 2 covers a wide range of controls that are a superset of the security concerns and requirements found in the various FDA regulations (CFR 21 Part 11, Part 820, GMP, etc.)

Maintaining our SOC 2 compliance ensures that our customers receive a highly available and secure solution that has been designed from the ground up to comply with various industry standard requirements, like CFR 21 Part 11. It also certifies the service is under strict change management controls to ensure the production service has successfully passed several layers of automated and manual testing before deployment. This testing, completed by Leading2Lean, can be used as a foundational layer of our customers own validation testing. This reduces the needed validation efforts of the customer, as major versions of the software are released, by leveraging our internal testing efforts.

How does cloudDispatch comply with Part 11?

CHAPTER 1--FOOD AND DRUG ADMINISTRATION	
DEPARTMENT OF HEALTH AND HUMAN SERVICES	
SUBCHAPTER A--GENERAL	
Subpart B--Electronic Records	
Sec. 11.10 Controls for closed systems.	*How Leading2Lean cloudDispatch Complies*
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:	The cloudDispatch system provides user level security designed to ensure records created or modified in the system maintain system authenticity, integrity, and restricts access by user role to provide confidentiality where necessary.
a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Dispatch uses leading industry technology in its core platforms and enforces referential integrity and consistency in multi-user environments. User entered information is tracked within the system, including IP addresses, usernames, and date/time information for data modifications.
(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 cloudDispatch records are available to authorized users in multiple query forms. Direct data dumps can be scheduled by request to the Leading2Lean administrator.
c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Records are retained for the life of the customer's subscription and in accordance with our Data Retention policy found at: https://support.leading2lean.com/hc/en-us/articles/115004658788-Data-Retention
(d) Limiting system access to authorized individuals	Dispatch security requires individuals to login with a valid username and password to access system. Additional IP address level restrictions can be enabled to further limit how authorized individuals can access the system.
(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	cloudDispatch uses secure, computer-generated, time-stamps on data records and provides a change history audit trail to track changes to dispatch records.

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.	
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The system enforces that only administrator defined events and action steps are permitted by the system.
(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.	Only authorized individual user logins are permitted to login and modify data.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	All input is validated at the data entry screen.
(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.	Leading2Lean provides training for all users of the system as part of the implementation process.
(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.	Use of the cloudDispatch system creates a visible feedback system to ensure users maintain accurate records in the system.
(k) Use of appropriate controls over systems documentation including:	
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	The cloudDispatch document revision control functionality provides standard process controls for authoring and controlling access to system operation and maintenance documentation.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	The cloudDispatch documentation functionality maintains revision control of documentation and provides an audit trail for all changes.
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 11.10, as appropriate and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary	All access to system data is secured by valid user logins and is restricted by security roles to ensure record authenticity, integrity, and confidentiality. Documentation uploaded to the cloudDispatch document revision control functionality is stored using encryption at rest technology. Additionally documents can be encrypted by the user before unloading as an extra measure of security.

under the circumstances, record authenticity, integrity, and confidentiality.	
Sec. 11.30 Controls for open systems.	
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	Dispatch user authentication is used to identify the user who is modifying data. Access requires both a valid username and password specific to the user.
(1) The printed name of the signer;	Yes, present in the record as history
(2) The date and time when the signature was executed; and	Yes, present in the record as history
(3) The meaning (such as review, approval responsibility, or authorship) associated with the signature.	The document center revisions and change control functionality provides an audit trail for authoring, review, approval, and publishing of documents.
(b) The items identified in paragraphs (a)(l), (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).	All records contain user login information and modification dates that are in a human readable form for electronic display or printout.
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.	All records contain user login information and modification dates that are in a human readable form for electronic display or printout. Users of the system have no ability to falsify, excise, or copy by ordinary means.
	[Code of Federal Regulations], [Title 21, Volume 1} [Revised as of April 1, 2012}, [CITE: 21CFR11}
Sec. 11.100 General requirements.	
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Access requires a username and password. System administrators have the ability to assure this is unique to each individual.
(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.	Our customer's trained administrator makes any changes to users or passwords and can assure compliance.
(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.	This is normally part of an internal SOP used to define your quality system. We work closely with your internal IT or responsible person to assure compliance is assured.
(1) The certification shall be submitted in pa per form and signed with a traditional handwritten	Part of internal SOP

signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, 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.	Part of internal SOP
Sec. 11.200 Electronic signature components and controls.	
(a) Electronic signatures that are not based upon biometrics shall:	
(1) Employ at least two distinct identification components such as an identification code and password.	Yes, access requires both and specific access to areas to view, add or change are defined for each user account.
(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 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.	We work with you to define which records require such signature and provide appropriate prompts to satisfy this requirement.
(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.	If the user's session is terminated due to inactivity, they must re-login using their username and password ensuring the integrity and authenticity of their digital signature.
(2) Be used only by their genuine owners; and	Yes
(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.	Yes
(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
Sec. 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:	We encourage a standard internal change process for any user or employment changes.
(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.	Yes, inherent in the system is the requirement that all usernames are unique.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Yes, controlled by customer's cloudDispatch administrator.

(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.	Yes, controlled by customer's cloudDispatch administrator.
(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.	Yes, Leading2Lean operational delivery teams monitor and report unauthorized attempts or denial of service.
(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.	Yes, controlled by customer's cloudDispatch administrator.

Conclusion

Based on the interpretation of FDA Title 21 CFR Part 11 rule of the U.S. Food and Drug Administration and the functions and features discussed within this document, Leading2Lean believes the cloudDispatch SaaS solution version currently being deployed in November 2018 as a managed service technically complies with the intent and requirements of the Part 11 rule.

References

FDA Regulatory Information:

https://www.fda.gov/RegulatoryInformation/default.htm

CFR 21 Part 11, Electronic Records; Electronic Signatures – Scope and Application:

https://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm

CFR 21 Part 11 Electronic Records and Electronic Signatures, Revised April 1, 2018

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1

CFR 21 Part 820, Quality Systems:

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820&showFR=1

Sec. 820.180 General requirements.

Sec 820.180 Subpart M - Records

Appendix 1: Example Test Validation Scripts

The following are example test validation scripts for covering the basic Electronic Records, Electronic Signatures, and Audit History functionality described above.

Test 001 – SUCCESSFUL LOGIN TEST					
Step	**Step Description (Procedure)**	**Expected Results**	**Actual Results**	**Pass/Fail**	**Initial/Date**
1.	Open browser Browse to https://<customer>.leading2lean.com Enter an existing username and the correct password into the login form Verify the browser redirects to the home / main menu screen. Verify the username listed in the upper right corner of the screen is the same as the one used to login.	User is able to login to the system and see the home screen.	Did the user successfully login to the home screen? ___ Yes ___ No Attachment #_____	___ Pass ___ Fail	

Test 002 – UNSUCCESSFUL LOGIN TEST					
Step	**Step Description (Procedure)**	**Expected Results**	**Actual Results**	**Pass/Fail**	**Initial/Date**
1.	Open browser Browse to https://<customer>.leading2lean.com Enter an existing username and the wrong password into the login form Verify the browser displays an error message and stays on the login screen.	User is unable to login to the system.	Was the user unable to login? ___ Yes ___ No Attachment #_____	___ Pass ___ Fail	
2.	Open browser Browse to https://<customer>.leading2lean.com Enter a non-existing username and a password into the login form Verify the browser displays an error message and stays on the login screen.	User is unable to login to the system.	Was the user unable to login? ___ Yes ___ No Attachment #_____	___ Pass ___ Fail	

Test 003 – CREATE DUPLICATE USER ACCOUNT TEST					
Step	Step Description (Procedure)	Expected Results	Actual Results	Pass/Fail	Initial/Date
1.	Login to cloudDispatch using a user account with Administrator privileges. Go to Setup Menu, then Users, click Add New link. Type in an existing username and fill out the rest of the fields. Click the Save Button. Verify the browser displays an error message and does not save the record.	Administrator is unable to create a duplicate user account in the system.	Was the administrator able to setup a duplicate user account? ___ Yes ___ No Attachment #_____	___ Pass ___ Fail	

Test 004 – INACTIVE USERS CAN'T LOGIN TEST					
Step	Step Description (Procedure)	Expected Results	Actual Results	Pass/Fail	Initial/Date
1.	Login to cloudDispatch using a user account with Administrator privileges. Go to Setup Menu, then Users, click on a user to edit. Uncheck the Active checkbox and click the Save Button. On a separate computer, have that user try to login to the system to verify the browser displays an error message and does not allow them access.	The inactive user can't login.	Was the inactive user unable to login? ___ Yes ___ No Attachment #_____	___ Pass ___ Fail	

Test 005 – CREATING/EDITING A DISPATCH CREATES ACCURATE DISPATCH CHANGE HISTORY					
Step	Step Description (Procedure)	Expected Results	Actual Results	Pass/Fail	Initial/Date
1.	Login to cloudDispatch using a user account with Resource privileges. Go to the "ALL" Dispatch screen, then click the New Dispatch link at the bottom of the screen. Fill in the appropriate fields and click Create Dispatch. Verify the Dispatch is listed on the main dispatch screen and contains the same information as entered above.	User can create a Dispatch in the system and it retains the correct information including the correct submitted by user account.	Was the Dispatch information correct as entered, including the correct submitted by user account? ___ Yes ___ No Attachment #_____	___ Pass ___ Fail	

	Click the Dispatch number link to edit the dispatch. Verify the information displayed in Dispatch Update screen is the same as entered above, including the submitting by field being set to the currently logged in user account.				
2.	Using the above Dispatch, from the Dispatch Update screen click the Dispatch Change History button at the bottom of the screen. Verify that the correct user and IP address is listed as the user that created the Dispatch.	The Dispatch Change History correctly identifies the user who created the dispatch.	Was the Dispatch Change History correct? ___ Yes ___ No Attachment #_____	___ Pass ___ Fail	
3.	Using the above Dispatch, edit the dispatch from the Dispatch update screen and click the Save Button. Click the Dispatch Change History button at the bottom of the screen. Verify that the changes to the dispatch are correctly reflected and attributed to the correct user.	The Dispatch Change History correctly identifies the edits to the dispatch and which user made them.	Was the Dispatch Change History correct? ___ Yes ___ No Attachment #_____	___ Pass ___ Fail	