Information Sheet
TraceGains FDA Title 21 Code of Federal Regulations (CFR) Part 11 Compliance

Introduction

This document describes how the TraceGains software platform facilitates compliance with the regulations defined by the Food and Drug Administration's Title 21 CFR Part 11 ("Part 11") for electronic records and electronic signatures.

The term "TraceGains software platform" refers to the following TraceGains modules: Supplier Management, Supplier Compliance, Audit Management, Specification Management, Formula Management, and Quality Management.

Part 11 Background

Part 11 went into effect on August 20, 1997. All companies serving industries regulated by the FDA must follow the regulations included in Part 11.

Part 11 refers to the FDA's regulations and procedures put in place to ensure accuracy, reliability, authenticity, availability, and integrity of electronic records and electronic signatures for persons and companies using Open and Closed systems to create, modify, maintain, archive, retrieve, or transmit electronic records.

To ensure Part 11 compliance, companies that manage records electronically are required to have controls in place to validate the consistency and accuracy of the intended functionality of the system, to safeguard against alterations or falsifications of records or electronic signatures.

Notice on Compliance

TraceGains customers often ask if a software vendor "complies" with Part 11. A software vendor and its associated products cannot, by themselves, be compliant.

TraceGains customers must adhere to Part 11 and the TraceGains software platform can only provide a product which has the features and architecture necessary to support customer compliance. Customer compliance with Part 11 is determined by how that customer implements and utilizes the TraceGains software platform. Customer compliance requires the implementation of management and procedural controls, including, but not limited to, notifications, training, standards operating procedures (SOPs), and disciplined administrative governance.

Each TraceGains customer will implement the TraceGains software platform differently, reflecting their business processes and requirements. The TraceGains software platform is a highly flexible and configurable solution that supports customer compliance with Part 11 regulations without the need to customize the software. The TraceGains software platform has the necessary functionality to enable TraceGains customers to comply with Part 11 regulations.

The TraceGains Software Platform and Part 11

The TraceGains software platform includes a suite of security, record management, and audit features that, along with the platform network and database security features, can be used to prevent unauthorized access to data and configuration information and to record actions taken to delete or modify such information.

The following content on this information sheet details, on a section by section basis, how the TraceGains software platform supports customer compliance with Part 11.

To review Part 11 further, please use this hyperlink: FDA Guidance Document

Definitions

The TraceGains software platform is an **Open System**. As such, customers of TraceGains must comply with controls applicable to both Closed and Open Systems as specified by Part 11.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Controls for Closed Systems (Title 21 CFR Part 11 Section 11.10)

11.10 Controls for Closed Systems			
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	System validation	**TraceGains** • TraceGains maintains quality controls related to the development, maintenance, and support of the TraceGains software platform, including both robust human quality assurance review protocols as well as regular, automated quality and performance analyses. This dual application of human and software quality review supports regular testing and validation of the accuracy, reliability, integrity, availability, and authenticity of TraceGains software platform features. • TraceGains software platform modules and sub-modules include audit trails that capture initial data values for records and subsequent changes thereto. TraceGains enables highly secure and configurable access controls related to different users' ability to access modules and sub-modules as well as create, read, update, and delete data fields associated with record data values. • Regular software updates applied automatically to the TraceGains software platform do not modify or delete customer records and the data associated with the records. **Customer** • Customers must configure access controls related to different users' ability to access modules and sub-modules as well as create, read, update, and delete data fields associated with record data value. • Customers may configure data fields in the TraceGains system to control the data, type of data, and/or format of data users may input to help ensure record accuracy and consistency. Records may only be accessed through the TraceGains software platform and such access is controlled by the customer's platform administrator.
11.10(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 FDA.	Record generation and copying	**TraceGains** • TraceGains enables user to generate accurate and complete copies of records in human readable and electronic form (in the PDF format) suitable for inspection, review, and copying by the FDA. • TraceGains automatically backs up all electronic records, enabling their protection and accurate and ready retrieval throughout record retention periods. • The TraceGains software platform also provides standard reporting capabilities to query data and generate reports in human readable and electronic format. **Customer** • Customers should establish an SOP for handing over electronic records to the FDA for inspection.
11.10(c)	Protection of records enable their accurate and ready retrieval throughout the records retention period	Record protection	**TraceGains** • All records created in the TraceGains software platform are stored in a secure database. • The TraceGains software platform database includes backups of all records and associated data in the system. • The TraceGains software platform provides data archiving features that also help to optimize system performance. These features provide long term storage capabilities, as well as protection, for records and associated data.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Controls for Closed Systems (Title 21 CFR Part 11 Section 11.10) (continued)

11.10(d)	Limiting system access to authorized individuals	Access limitation	**TraceGains** • Access to the TraceGains software platform is limited to authorized users established by the user administrator. • Authorized users are provided unique usernames and one-time passwords upon account creation. • User passwords are not stored in the database; a hash key for the password is created and stored in an encrypted form and passwords are authenticated against the key. • The TraceGains software platform has a session lock for failed login attempts. Access is revoked after a defined number of consecutive failed login attempts. • TraceGains also automatically logs users out of the software platform after a defined time period for which the user's session is left idle, requiring re-authentication when the user returns. **Customer** • User administrators may limit the actions that authorized users may perform in the platform by defining the roles and permissions for authorized users. • Customers are responsible for setting and maintain unique usernames and passwords after account creation.
11.10(e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries 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.	Audit trails	**TraceGains** • Audit trails are available system-wide or for individual records and/or items on the TraceGains software platform. Each audit trail includes the date, the time, the performed action, and the User ID who performed the action. Additional audit trails are available for system activity (e.g. user login, failed access attempts). • The TraceGains software platform includes a full audit trail of record additions and changes within the TraceGains database. • Audit trails within the TraceGains software platform are secure and cannot be modified using ordinary means. The audit trail is backed up in the same way as records and data associated with records in as described in 11.10(c). **Customer** • Customers are responsible for ensuring that system clock dates and time stamps are accurate and secure from tampering.
11.10(f)	Use of operational system checks to enforce permitted sequencing steps and events, as appropriate	Operational system checks	**TraceGains** • The TraceGains software platform includes both standard and user-configurable enforced sequencing steps and events. **Customer** • In most cases, the sequencing of steps and events is determined and configurable by the customer. • The customer is responsible for ensuring that the sequencing of steps and the associated checks are properly configured for each process.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Controls for Closed Systems (Title 21 CFR Part 11 Section 11.10) (continued)

11.10(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	Authority checks	**TraceGains** • TraceGains ensures that each authorized user is assigned a unique user ID and password, token, or SSO account and will only allow authorized users to access the TraceGains system after authentication with valid credentials. • User controls in the TraceGains software platform are supported by: unique user ID and password, user role configuration with associated permissions and access controls; password duration and expiration; and disabling of user accounts. • Only an authorized user can electronically sign a record and can create, read, update, or delete (CRUD access) specific types of information. CRUD access is configurable by user role and may be applied across system modules. **Customer** • User administrators are responsible for assigning different user roles and permissions to authorized users, including but not limited to CRUD access.
11.10(h)	Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction	Device/ terminal checks	**TraceGains** • The TraceGains software platform is a SaaS, fully web-based software package. It may be delivered through a customer's corporate Intranet. **Customer** • External access at the device level is controlled by the customer through user access controls (e.g., unique usernames and unique passwords) as well as, for example, through firewalls and VPN administration. • Authorized users with necessary permissions may further configure additional checks on data field entries using configurable business rules and workflow features.
11.10(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	Training and user accountability	**TraceGains** • TraceGains employees who develop, maintain, and test the TraceGains software platform are trained to perform their assigned tasks. • TraceGains' Customer Success Team provides training during customer onboarding and configuration. If further training or education is required, TraceGains can provide module- or system-specific training for additional fees. • TraceGains supports ongoing user learning and application mastery via the TraceGains Academy, where users may conduct trainings and receive associated badges for no additional charge. **Customer** • Customers are responsible for ensuring their users are adequately trained to use the TraceGains platform and on the customer's SOPs regarding electronic records and electronic signatures. • Customers may assign users to specific roles within the TraceGains software platform that limit that user's access (and associated CRUD permissions) within the platform (per 11.10(g) above).

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Controls for Closed Systems (Title 21 CFR Part 11 Section 11.10) (continued)

11.10(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		**Customer** • This clause is a procedural requirement that must be met by the customer and is not related to the functionality of the TraceGains software platform.
11.10(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 2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation	System document control	**TraceGains** • TraceGains provides official documentation for the operation and maintenance of the TraceGains software platform. • Release-specific software information is distributed when the TraceGains software platform is updated. • The TraceGains software platform development team follows design and control processes for creation and tracking of relevant documents. • Changes to official TraceGains software platform documentation are revision controlled and recorded. **Customer** • Customers are responsible for ensuring that appropriate controls are maintained over the distribution and access to TraceGains documentation.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Controls for Open Systems (Title 21 CFR Part 11 Section 11.30)

11.30 Controls for Open Systems			
11.30	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 under the circumstances, record authenticity, integrity, and confidentiality.	Controls for Open Systems	**TraceGains** • The TraceGains software platform is a SaaS, cloud-based solution. All customers of TraceGains receive regular updates to their platform with the newest features, performance enhancements, and fixes. • The TraceGains software development process is controlled through internal processes governing the security and quality of all features, performance enhancements, and fixes. Quality control is a central part of the TraceGains software development process as further defined within Section 11.10a. All new features, performance enhancements, and fixes undergo quality review to ensure their application to the TraceGains software development platform will not compromise the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. • Access to customer instances of the TraceGains software platform for customer support (as defined in TraceGains' master services agreement) is gated and restricted to defined individuals who must follow internal procedures governing access. • The TraceGains software platform includes data encryption.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Signature Manifestations (Title 21 CFR Part 11 Section 11.50)

11.50 Signature Manifestations			
11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: 3. The printed name of the signer; 4. The date and time when the signature was executed; and 5. The meaning (such as review, approval, responsibility, or authorship) associated with the signature	Signature manifestations	**TraceGains** • Specific records in the TraceGains software platform include default signature requirements (users must enter their password, which is associated with their name and the date of the action), including approvals on Specifications in the Specification Management system, approvals on Formulas in the Formula Management system, approvals on Item Data Sheets, and approvals on documents within the Document Authoring module of the Quality Management system. • The TraceGains system allows Customers to apply signature requirements on records in addition to the above-listed record types. These signature requirements applied to additional records may be configured to be required upon any modification to a specified record type by a user or upon a modification to a pre-determined sub-set of fields within a specified record type by a user. • Electronic records in the TraceGains software platform clearly indicate the full printed name of the signer, the date and time the signature was executed, and the meaning of the signature (e.g. review, approval, responsibility, or authorship). **Customers** • Users are responsible for accurately configuring the meaning of each signature applied and accurately configuring any additional signature requirements on Customers' desired record types. • Users are responsible for accurately configuring automated data update tools within the TraceGains platform (e.g., APIs, business rules) to not automatically update records where user policies and procedures require user signature prior to modification.
11.50(b)	The items identified above 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)		**TraceGains** • Electronic signatures are stored in the electronic records to which they are applied and may be included in the printout or display of the record.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Signature/Record Linking (Title 21 CFR Part 11 Section 11.70)

11.70 Signature/Record linking			
11.70	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	Signature/ record linking	**TraceGains** • Electronic signatures on the TraceGains software platform are linked to their respective electronic records to ensure that the electronic signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. • The TraceGains software platform identifies to the user whether a record has been modified after electronic signature. Modification after electronic signature requires user application of a new electronic signature. Updated records with new signatures applied are linked to the original signed records and previous versions thereof. • The user ID of users who complete electronic signatures is linked to the respective electronic records; this association prevents the signature from being excised. The password component of the electronic signature is not stored with the record to prevent that electronic signature from being copied or transferred.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Electronic Signatures (Title 21 CFR Part 11 Section 11.100)

11.100 Electronic Signatures			
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else	Unique electronic signatures	**TraceGains** • All electronic signatures are unique to each individual unique user ID. • If a user ID is deactivated, another user with the same user ID cannot be created. **Customer** • Customers are responsible for ensuring that no two or more users share the same user account.
11.100(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	Verification of identity	**Customer** • This clause is a procedural requirement that must be met by the customer and is not related to the functionality of the TraceGains software platform.
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	Certification	**Customer** • This clause is a procedural requirement that must be met by the customer and is not related to the functionality of the TraceGains software platform.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Electronic Signature Components and Controls (Title 21 CFR Part 11 Section 11.200)

11.200 Electronic Signature Components and Controls			
11.200(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 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 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 signature components 2. Be used only by their genuine owners; and 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	Controls for electronic signatures	**TraceGains** • Electronic signatures in the TraceGains software platform are created based on a users' username and password. Each signing action is linked to one single electronic record and authentication of username and password is always required prior to signing. • The TraceGains software platform utilizes multiple password security features to ensure the highest level of limitation of system access. A user is required to input their username and password every time the user first logs into the system. Further, any session by a user within the platform that is left idle for a pre-defined period requires re-authorization when the user returns. After a user logs into the system, any subsequent electronic signatures required by the user will require that user to re-enter their password for additional security. • The TraceGains software platform enforces 1ii of Part 11 by forcing the user to log on with that user's username and password every time a new session is initiated. • The TraceGains software platform only allows the assigned user (genuine owner) to user their individual electronic signature. • User passwords are kept confidential and are unavailable to any other system user, including the system administrator. Password reset only enables the user to create a new, secure and confidential password. **Customer** • Customers are responsible for ensuring that signatures are only used by their genuine owners. • Customers are responsible for setting procedures to ensure that electronic signatures made by anyone other than the genuine owner requires such activity be done in the presence of one or more other individuals.
11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners	Biometrics	• N/A. TraceGains does not support biometric devices.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Controls for Identification Codes/Passwords (Title 21 CFR Part 11 Section 11.300)

11.300 Controls for Identification Codes/Passwords			
11.300(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	Unique ID/ password combinations	**TraceGains** • User IDs within the system are unique. • User passwords are kept confidential and are unavailable to any other system user, including the system administrator.
11.300(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password aging)	Password aging	**TraceGains** • Passwords expire after a defined period of time and password history controls limit password reuse.
11.300(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	Lost ID/ password management	**Customer** • Customer system administrators may disable user accounts or reset the password of any user. User passwords are kept confidential and are unavailable to any other system user, including the system administrator. This reset action only enables the user to create a new, secure and confidential password. • User administrators are responsible for disabling user accounts or resetting passwords if suspected unauthorized access occurs and for issuing temporary or permanent replacements using suitable rigorous controls.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.

Controls for Identification Codes/Passwords (Title 21 CFR Part 11 Section 11.300) continued

11.300(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	Controls to prevent unauthorized credential use	**TraceGains** • User accounts are automatically locked after a predefined number of unsuccessful login attempts. User login logs indicate the number of attempts.
11.300(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	Periodic testing of ID/password generation	**Customer** • This clause is a procedural requirement that must be met by the customer and is not related to the functionality of the TraceGains software platform.

Summary

The TraceGains software platform supports customer compliance with Part 11 requirements and includes a suite of security, record management, and audit features that, along with operating system and database security features, can be used to prevent unauthorized access to data and configuration information and to record actions taken to delete or modify such information.

Confidential | Copyright © 2021 TraceGains, Inc. All rights reserved.