Salesforce.com and the FDA's 21 CFR Part 11 Requirements

Validation Overview

June 2010

CONTENTS

DISCLAIMER

Please note: this document is intended for informational purposes only. Please bear in mind that:

- This document does not constitute legal advice, and should not be viewed as a substitute for advice by qualified counsel.
- Nothing in this document constitutes a warranty, representation, offer or proposal. Any purchase of salesforce.com services by you is subject to your entry into a definitive legal agreement with salesforce.com.
- Nothing in this document is a commitment to deliver any features or functionality. The development and timing of any features or functionality is at the sole discretion of salesforce.com.

OVERVIEW

Life sciences companies must comply with general FDA regulations related to the *qualification* and *validation* of systems. Qualification is a process that is used to evaluate whether a system complies with regulations, specifications, or conditions imposed at the start of a development phase. Validation is a process of establishing evidence that provides a high degree of assurance that a system accomplishes its intended requirements. Generally, infrastructure must be qualified, while applications must be validated. This document focuses on validation specifically related to "21 CFR Part 11" (The term *21 CFR Part 11* refers to the Code of Federal Regulations [CFR]: Title 21 – Chapter 1, Food and Drug Administration Part 11 – Electronic Records; Electronic Signatures), as opposed to the qualification and validation processes related to broader FDA regulations.

21 CFR Part 11 is part of the Code of Federal Regulations, which have been promulgated to enforce the law embodied in the Federal Food, Drug, and Cosmetic Act. Life sciences companies must comply with 21 CFR Part 11 if they want to take advantage of electronic records and "electronic signatures." The law applies to computer systems that are regulated by existing FDA regulations, also called predicate rules, as opposed to non-FDA-regulated business systems. The FDA also produces guidance documents to assist with interpretation and enforcement.

The 21 CFR Part 11 regulations created guidelines for the proper handling of FDA-regulated information that is stored electronically and the application of electronic signatures that are considered to be the legally binding equivalent to handwritten signatures on documents. Computer systems that maintain records electronically must ensure the integrity of the record and ensure that:

- the information gathered is accurate and complete
- there is accountability for actions that create, modify, or delete information
- a complete history of the record is available from point of inception
- electronic signatures on records cannot be repudiated.

Computer systems need to have adequate technical capabilities and features to permit organizations to meet the compliance requirements mandated by these regulations. Yet, the computer system used for any regulated business process is only one component of the regulated process. To determine that a process is compliant with the federal regulations, an organization must address not only the functions and features of the computer system used, but also how it is being deployed and configured, the intended use of the system, and the supporting processes and procedures for the application. **While Salesforce, in and of itself, is not a validated system, it has the native functions and features that, if implemented properly, enable the computer system owner to satisfy the compliance requirements of 21 CFR Part 11.**

Life sciences organizations can rely on salesforce.com's platform to perform the following functions in a manner that is compliant with the requirements in 21 CFR Part 11:

- store and access documents for review
- deliver information about clinical trials
- track regulatory applications
- track complaints and adverse events
- facilitate medical device field service
- manage samples
- manage records
- communicate and assign tasks
- monitor research and development
- control workflows and processes
- store and manage changes to standard operating procedures (SOPs).

This document provides an overview of *system validation*, a component of 21 CFR Part 11, as indicated in section 11.10(a) of the regulation, which states systems must be validated "to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."

COMPLYING WITH 21 CFR PART 11

Life sciences companies that have chosen to maintain records electronically must comply with 21 CFR Part 11 by ensuring that:

- the software products they use have been built / configured to function in a way that enables them to comply
- they develop and follow supporting SOPs that describe how to use and maintain the system in a way that enables them to comply.

21 CFR Part 11 regulations provide guidance for life sciences companies to meet the following goals:

- ensure the authenticity, integrity, and confidentiality of electronic records from the point of creation to the point of receipt by the FDA or point of lifecycle of retention of the record
- generate accurate and complete copies of records for the FDA to inspect and review
- ensure the security and easy retrieval of electronic records
- ensure that only authorized individuals can access, manipulate, and electronically sign records
- maintain a log of all changes made to electronic records throughout their lifecycle
- record and securely link electronic signatures to the electronic records to which they have been applied
- ensure that record processing steps are performed in the proper order
- ensure individuals who develop, maintain, or use the electronic record / electronic signing system are properly trained
- ensure individuals are accountable for actions initiated under their electronic signatures
- maintain control over system documentation
- establish and maintain controlled SOPs regarding all of the above and other requirements.

The regulations in 21 CFR Part 11 aim at reducing fraud while ensuring that electronic signatures and records are as reliable as their traditional paper counterparts.

VALIDATING CLOUD SYSTEMS

Overview

Cloud-based systems such as salesforce.com can be validated just as on-premise or hosted software can be validated. However, these processes differ. Salesforce.com, for example, manages the infrastructure and hardware associated with a customer's system. Salesforce.com is responsible for controlling and qualifying the infrastructure, while customers are responsible for validating the entire system. Furthermore, salesforce.com provides three releases per year whereas on-premise vendors typically provide releases much less frequently.

The purpose of system validation, according to The General Principles of Software Validation (FDA 2002), is to provide "confirmation by examination and provision of objective evidence that computer system specifications conform to user needs and intended uses, and that all requirements can be consistently fulfilled", and from the Part 11 context "to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records." Validation provides documented evidence that processing activity and electronic records for a particular system and intended use are accurate and can be trusted.

Validation includes the hardware, software and operational environment for the entire system in question. Not all systems require validation. Life science companies must validate any system that creates, modifies, or maintains data in electronic form that meets the record-keeping requirements of any FDA regulation.

In either an on-premise or cloud-based environment, validation requires a company's business, compliance and IT groups to answer three key questions to establish a system's fitness for use:

- Can I prove the system was installed correctly? (see *IQ – Installation Qualification*)
- Can I prove the system is operating correctly? (see *OQ – Operational Qualification*)
- Can I prove the system is performing correctly to meet the stated user requirements? (see *PQ – Performance Qualification*)

The processes required to answer these questions differ in an on-premise versus a cloud-based environment. The key difference pertains to how the infrastructure and platform is controlled in each environment.

Salesforce.com uses a technology layer and a metadata abstraction layer. Salesforce.com controls the technology layer, so that when upgrades take place, only this layer is affected, as opposed to the layer containing customers' metadata. Unlike on-premise systems, salesforce.com does not remove custom fields or objects; instead, its core modules apply incremental value by adding new or additional value-add features and functions.

Validation Approaches

Companies use several different approaches to validation. Any approach should leverage existing documentation (e.g. documentation available from salesforce.com) in order to make efficient use of resources. In addition, based on current regulatory initiatives and industry trends (most notably Pharmaceutical Current Good Manufacturing Practices (CGMPs) for the 21st Century, August 2002), the approach should incorporate a risk-based strategy for computer systems validation. That is, a company must ascertain the relative risk associated with a system, and its data, when deciding an appropriate approach to validation (see also GAMP5® and ICH Q9). Companies are encouraged to take a holistic approach to validation, looking at the process in its entirety, and well as its individual components.

One of the most popular validation processes includes three primary activities: Installation Qualification (IQ), Operational Qualification (OQ) and Performance Qualification (PQ).

Installation Qualification (IQ)

- *What it is:* IQ is a controlled, documented activity, typically embodied with an approved test protocol, which ensures all software and hardware is installed correctly.

- *On-premise IQ:* In a on-premise environment, IQ requires the recording of a system's standard pieces of information, including model, type, configuration, equipment location, installed software version and serial number of the computer(s) on which the software is installed, as well as the operating environment within which the equipment resides. IQ activities can vary greatly company to company and there is no standard documentation process.

- *Cloud-based IQ:* In a cloud-based environment, it is unlikely that a customer will perform IQ on the underlying infrastructure. In the case that a customer does perform IQ on the salesforce.com infrastructure, one can document the proper installation and configuration of a system electronically or in hard copy. More likely, a customer will conduct a vendor audit to ensure that Salesforce or another cloud-based system has a quality management system in place, is following the customer's internal quality and testing practices, and has processes and procedures in place to keep the infrastructure and environment in a controlled state.

- *Frequency of IQ:* In an on-premise environment, IQ steps may need to be repeated every time a new piece of software or hardware is installed. In Salesforce, system updates are automatically pushed to customers multiple times per year, and customers are notified of the new functionality well in advance of the release to provide time for testing if necessary. No hardware or software must be reinstalled.

Operational Qualification (OQ)

- *What it is*: OQ is a controlled, documented activity, typically embodied within an approved test protocol, which tests to make sure system functionality is working as expected. For example, when a system is installed, OQ tests to make sure the application functions are operating as expected.

- *On-premise OQ:* In an on-premise environment, one must typically complete test scripts to demonstrate that the system is functionally operating correctly under normal operating conditions.

- *Cloud-based OQ:* In a cloud-based environment, one can write a script that, if written well initially, can be leveraged for future use. Additionally, scripts from the initial validation may be shortened and used to double-check information, as opposed to going through the process of testing core features again. In Salesforce metadata does not need to be updated, as this layer of data is left untouched.

- *Frequency of OQ:* In an on-premise environment, certain OQ steps may need to be repeated, or new tests generated, based on what additions or changes were applied during every new release. In Salesforce, companies may not need to complete an OQ multiple times because they may leverage initial scripts.

Performance Qualification (PQ)

- *What it is*: PQ is a controlled, documented activity, typically embodied within an approved test protocol, which demonstrates a system's ability to meet the owner's process requirements consistently and reliably over time. Owners typically execute PQ in the actual production operating environment, with trained users following approved procedures. Owners frequently test scalability in the PQ, such that when a system is scaled to a large number of users, the system functions correctly. PQ generally includes worst case scenarios and load testing as well.

- *On-premise PQ:* Using system scalability as an example, in an on-premise environment, one must test the system's hardware, operating system, and database to ensure that the system has enough memory to support scalability.

- *Cloud-based PQ:* Using system scalability as an example, cloud systems like Salesforce are immediately scalable. Since one of the purposes of PQ is to test the boundary by which the system (process) will be validated to operate, it will be up to the user to set (and test) the initial limit. When the owner needs to expand, a supplemental PQ (under change control) requires simple actions such as ensuring that field sizes are large enough.

- *Frequency of PQ:* In an on-premise environment, one must repeat PQ steps for each new release. In Salesforce, one essentially completes the PQ once, because Salesforce does not add fields or make changes to existing fields.

MAINTAINING THE VALIDATED STATE

Salesforce.com provides upgrades on a seasonal release schedule. When changes occur within both software and hardware, life sciences companies must ensure that these changes are conducted in a controlled fashion. A systematic approach to change control includes the following four steps: 1) identifying all changes, 2) completing a risk assessment of all changes, 3) determining how each change impacts the validated system and 4) testing, if required. If a change is low impact and low risk, testing may not be required, and only the appropriate documentation needs to be updated (e.g. functional specification). If a change is moderate to high impact and moderate to high risk, one must develop testing documents or re-execute testing documents.

When salesforce.com makes any changes to the core application, customers are notified well in advance of the actual release and can test new features in a sandbox. This ensures that:

a) new application features and changes to the existing implementation are evaluated and controlled prior to release to production

b) new features/changes to existing are properly tested

c) potential negative impacts to the production environment are proactively identified and resolved

d) the need for unexpected rollbacks can be reduced to an acceptable level.

If customers want to change their own specific configurations, they must complete these changes under their own change control processes.

Risk Assessments

Companies should have thorough knowledge of their business process, the platform/technology, and salesforce.com's development, testing, and release methods which should be used to perform risk assessments. A well-informed, risk-based decision making process must ultimately determine, for any regulated user, how much new testing, periodic regression, and/or modification to existing process controls will be required for each salesforce.com release. Companies that adopt cloud computing may find they lower their overall validation efforts but that they also must place greater emphasis on processes that can address the frequent release activities.

CLOUD-BASED VALIDATION SERVICES

Several third-party organizations including qPharma and ModelMetrics/CQV specialize in system validation and provide professional services to salesforce.com's life sciences customers. These organizations provide services such as:

- project management
- pre-validation planning
- training on regulatory requirements
- auditing and assessments
- testing
- SOP development and training
- requirements gathering, design specs, and templates, as well as traceability throughout the document and testing processes
- system development and configuration
- vendor and system selection
- implementation and retirement plans
- authoring and reviewing documentation and more.

CONCLUSIONS

Regulated companies can benefit from virtues of cloud computing and can use Salesforce in validated environments. Validation and the maintenance of the validated state of a salesforce.com system is, in essence, a de facto partnership between the regulated company and salesforce.com. Companies should embark upon use of salesforce.com with a full understanding of cloud computing, an understanding of the control, validation, and data integrity requirements, and the impact of the cloud computing on existing compliance perspectives and validation practices.

DETAILS OF THE FDA's 21 CFR Part 11 REQUIREMENTS

Authority: Secs. 201–903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321–393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).

Subpart A—General Provisions

§ 11.1 Scope.

(a) *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.*

(b) *This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also 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.*

(c) *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 excepted by regulation(s) effective on or after August 20, 1997.*

(d) *Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.*

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

§ 11.2 Implementation.

(a) *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.*

(b) *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:*

(1) The requirements of this part are met; and

(2) 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, 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.

§ 11.3 Definitions

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).

(2) Agency means the Food and Drug Administration.

(3) Biometrics mean 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.

(4) Closed system means an environment in which system access is controlled by persons who are responsible for content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication that is 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.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) 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.

(8) 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 instrument 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.

(9) 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.

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:

Based on Section VI Definitions (§ 11.3) 41.-, the agency states that the most important factor in classifying a system as closed or open is whether the people responsible for the contents of the electronic records control access to the system containing those records. A system is closed if access is controlled by people responsible for the contents of the records. Because customers control the access rights to their salesforce.com instance of the platform and to their records, customers are well founded in concluding that the salesforce.com platform critical criterion and may be qualified as a closed system for purposes of this legislation.

The salesforce.com platform may be qualified as an open system in the case of customers who utilize premier support with dedicated administration. The platform could also be qualified as an open system in the case of the "login as access" customer support feature, which allows customers to give temporary access to Salesforce personnel for the purpose of troubleshooting and resolving technical issues.

It is important to note that the FDA is gradually moving away from the "open" and "closed" system terminology.

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

In deploying Salesforce, salesforce.com recommends that customers implement policies and procedures that include a periodic audit of the production system to ensure accuracy, reliability, and consistent intended performance in the installed active environment. Salesforce.com is available to assist FDA-regulated customers that have the staff available to quickly and effectively perform their own validation, depending on the applications they use or create on the salesforce.com platform. Audit logs and change-history tracking provide for automatic data and user name assignment to entries and edits in the history log, enabling tracking and accountability. The use of both create and edit time stamps allows any changed records to be readily detected. (*Please see "Validating Cloud Systems" for more detailed information.)*

(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.*

Salesforce.com applications provide extensive reporting capabilities, so reports can be generated to satisfy regulatory needs. Reports can be generated in both electronic and hard copy form, and once created, can be locked down to prevent manipulation of all data output. Data stored within the platform can be exported in a variety of formats for the purposes of review, audit, and archive. Such formats include CSV, PDF, XML, and more.

(c) ***Protection of records*** *to enable their accurate and ready retrieval throughout the records retention period.*

All electronic records, as well as audit trail logs and any reason for change records, are maintained in the secure multitenant database of the salesforce.com platform. Access to the data is limited to specific individuals or groups. The modification and / or deletion of records is restricted, to ensure integrity throughout the record retention period; audit trail is also available for deletions. Salesforce does not contain an archiving mechanism. All records and associated audit trails are available for retrieval

/ data export until they are deleted from the Salesforce repository, and customers control deletion. Salesforce.com recommends that customers develop policies and procedures covering records retention (how long a record should be maintained) and disposition (what is done with the record at the end of its lifecycle). The policy should include specific rules for deleting, purging, or archiving records at the end of their lifecycle. Salesforce.com can assist in the development of these policies and procedures as well as in system configuration.

Salesforce.com also has robust data backup and disaster recovery mechanisms in place. In addition to a disaster recovery site, Salesforce allows customers to download and back up their data each week through a weekly export feature.

(d) ***Limiting system*** *access to authorized individuals.*

All electronic records, as well as audit trail logs and any reason for change records, are maintained in the secure multitenant database of the salesforce.com platform. Record access is controlled by use of a unique sign-in (username) and password pair. Multiple levels of security and limitation of access to records and functionality are based on user roles, organization, and responsibilities. Salesforce.com recommends that customers implement policies and procedures to control the circumstances under which system access is granted as well as the user roles that define such access.

Salesforce monitors and logs all access attempts, recording the username used, the date and time of the access attempt, and whether the attempt was successful or not. Customers can configure their systems to set a lock out after a certain number of failed access attemps.

(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 as long as it is required for the subject electronic records and shall be available for agency review and copying.*

All electronic records (objects) contain a minimum of two date and time stamps: creation date and last modified by date and time. Time stamps are pulled from a common server. Each Salesforce data center has a network time protocol server that is synchronized to all production systems.

Also, all electronic records contain information identifying the user who created or modified the record. When an electronic record is changed, the date, time, and action

are recorded, along with both the previous and changed field values, which are recorded in fields flagged for audit history. All audit trail records are maintained and can be archived for maintenance and stored for the required time periods.

Change-history tracking provides for automatic data and user name assignment to entries and edits in the history log, enabling tracking and accountability. The system is also flexible in that customers can add their own custom data elements to the audit trail.

(f) ***Use of operational system checks*** *to enforce permitted sequencing of steps and events, as appropriate.*

The salesforce.com platform data collection and maintenance operations are managed through a well-defined sequence of steps (workflow) as defined by the project or system administrator. These workflow steps limit operators or users to specific functions and controlled entries or responses. Process control (workflow) events and violations are managed through additional workflow sequences, to ensure proper compliance throughout a process. Salesforce workflows can be used to ensure that the sequence of events prescribed in the customer's policies and procedures for a given process is strictly observed.

(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 salesforce.com service maintains a list of users, roles, and access rights within its multitenant database. User authentication is provided by a unique sign-in and password maintained within the database (system configurable).

- All passwords are encrypted within the database.
- Password complexity requirements can be set by customers to inhibit the use of weak passwords.
- Password aging can be set to forces users to change passwords after a specified period of time.
- Password recycling configuration can be set to inhibit users from reusing a password for a specified period of time.
- Automatic account lockout can be set to guard against unauthorized use.
- Automatic sign-out after a specified idle period can be set to force additional sign-in to continue system access.

- Salesforce.com also provides Single Sign On via federated authentication using SAML or delegated authentication.

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

Programmatic access to data for purposes of entry or retrieval of data is controlled by both a user name / password combination (a session ID) and a client ID code that further identifies the programmatic instructions for accessing the data in the system. Both identifiers may be required for successfully accessing the system remotely. Remote access can be further constrained, with only certain IP addresses (terminals) being permitted to access the system. This makes it possible to verify that requests are coming from known and authorized remote terminals. Salesforce.com recommends that customers develop policies and procedures for both remote and programmatic access to their data repositories.

(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.*

Salesforce.com provides a variety of training and educational services tailored to meet the requirements of the various categories of users who will utilize the salesforce.com platform. Additionally, salesforce.com works closely with clients to customize training classes based on their specific needs. Conformance with this requirement is the responsibility of the customer.

(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.*

Salesforce.com recommends that customers implement policies and procedures to cover the actions that administrators and end users must perform when using the Salesforce system. For administrators, policies and procedures should be developed for system-related actions such as user and group management, password management and audit trail configuration, archiving, and purging. For individual users, policies and procedures should be developed for actions such as data entry and data updates.

Conformance with this requirement is the responsibility of the customer.

(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.

Salesforce.com provides and maintains documentation for the salesforce.com platform in electronic form. This documentation should be included in part or in whole with the customer's own specific systems documentation.

Salesforce.com recommends that customers develop policies and procedures covering the control of system operational documentation, system maintenance schedules and update activities.

---

§ 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 under the circumstances, record authenticity, integrity, and confidentiality.

Based on Section VI Definitions (§ 11.3) 41.-, the agency states that the most important factor in classifying a system as closed or open is whether the people responsible for the contents of the electronic records control access to the system containing those records. A system is closed if access is controlled by people responsible for the contents of the records. Because customers control the access rights to their salesforce.com instance of the platform and to their records, customers are well founded in concluding that the salesforce.com platform critical criterion and may be qualified as a closed system. However, in certain circumstances, it may also be classified and qualified as an open system. When a customer has premier support with dedicated administration, the system can be qualified and classified as open. In these cases, the additional controls required by open systems are required for the salesforce.com platform.

Salesforce.com addresses the controls that customers must put in place for open or closed systems. Salesforce.com recommends that an organization implement usage policies and procedures to satisfy this requirement. Salesforce provides user authentication, data integrity, and confidentiality as follows:

- Authentication: System access is controlled through the use of usernames and passwords. For more information, see the response to Requirement 11.10 (d).

- Integrity: Users with appropriate permissions may add and update records appropriate to their level of permissions. Each activity is audited, and the values of the record prior to an update are recorded in the audit history for that record. The ability to delete an object can be strictly controlled through the use of record- and field-level permissions. Change-history tracking provides for automatic data and user name assignment to entries and edits in the history log, enabling tracking and accountability.

- Confidentiality: To ensure confidentiality, Salesforce is deployed in a secure communications network employing the Secure Sockets Layer (HTTPS) security mechanism, which encrypts the data stream between the browser and the server. Configuration access can be limited to a specific, predefined set of users and IP addresses. Access permissions are extremely granular and extend to individual fields within any record in the system. The owner of an object or a record (or another authorized user) can modify the permissions to restrict access to confidential records. For more information, see the response to Requirement 11.10 (g).

- Digital Signatures: Salesforce.com provides an AppExchange component that supports digital signatures. This component can be installed into a customer's Salesforce account. For more information, see the response to Requirement 11.50. Salesforce does not directly support biometric devices such as fingerprint recognition and retinal scanning.

---

§ 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.

Signature objects can be added to any salesforce.com application. Both types of signature objects are based on a user's being authenticated by a unique sign-in and password maintained within the database. For example, here are two types of signature objects that can be used.

All Reason for Change signature objects could provide the following information:

- User name
- Employee name
- Date/time of the signing
- Reason code
- Free-form comment.

All Process Event signature objects could provide the following information:

- Employee name (event)
- Date/time of the event
- Type of event
- Employee name (assignable cause)
- Date/time of the assignable cause
- Assignable cause code
- Employee name (corrective action)
- Date/time of the corrective action
- Corrective action code
- Free-form comments.

(b) *The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).*

The salesforce.com platform provides extensive reporting capabilities, so this information can be supplied in human-readable form. These reports can also be viewed on-screen (on a computer display) or printed out. Reports incorporating a signature object associated with any record can be displayed. For more information, see the response for 11.10 (d).

---

§ 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 within Salesforce are linked to the user who created or modified the record. Audit-trail / change-history records cannot be deleted or modified in any way from the salesforce.com applications. The user object cannot be disassociated from the original record or re-associated to another record.

Subpart C—Electronic Signatures

§ 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.*

Each Salesforce user is identified by a unique identifier in the database that cannot be deleted or removed but whose further use can be disabled. These unique identifiers are linked, thereby identifying the user who created or modified a record. As a further security measure, new users are required to specify a unique password during their first use of Salesforce. This ensures that the users, and no one else (not even the administrator), know their password.

Salesforce.com also recommends that customers implement policies and procedures to ensure that a given username is assigned to only one individual, that all individuals set their own password at the first login, and that all individuals agree not to divulge their password under any circumstances. For more information, see the response to Requirement 11.10 (d).

(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.*

As part of the deployment of Salesforce, salesforce.com recommends that the deploying organization implement policies and procedures to ensure that usernames are assigned to individuals with proper authorization and approval from their superiors.

Conformance with this requirement is the responsibility of the customer.

(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 and equivalent to traditional handwritten signatures.*

Salesforce can list the group of users in an organization who have the signing authority previously described. A Salesforce report can then be generated to provide the FDA with a list of the users who are authorized to apply electronic signatures. A standard operating procedure coupled with workflow elements and templates within Salesforce can be designed to manage this process and generate the appropriate correspondence to be sent to the FDA. Such correspondence would attest to the legally binding equivalence of users and their electronic signatures.

Conformance with this requirement is the responsibility of the customer.

---

(1) The certification shall be signed with a traditional handwritten signature and submitted in paper form 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

§ 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.

A unique login name and password are required for gaining access to the Salesforce system. These two items uniquely identify a Salesforce user, and that person's name is subsequently associated with every record transaction performed by that user. The initial login to the system is considered the first signing.

(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 electronic signature components.

Salesforce requires the entry of all signature components (username and password) at first sign-in. Where a signature action is required, re-entry of the User ID and Password signature components can be added, based on the application processes. An example might be to require the user to re-authenticate (e.g. enter User ID and Password as a signature execution action) before saving entered or reviewed data.

Automatic sign-out requirements (forcing a subsequent sign-in) can be implemented, based on a predetermined time of inactivity or completion of a data entry operation. In this case, the subsequent sign-in counts as a new first signing.

Salesforce also includes a new customer-configurable feature called Captcha, which ensures an additional level of authentication.

---

(2) Be used only by their genuine owners; and

Security measures built in to the Salesforce system help ensure that an electronic signature is used only by its actual owner. These measures include password aging, password recycling, idle account lockout, retry lockout, and password encryption.

Training of users on the appropriate safeguards and use of passwords is fundamental to the integrity of their use. Non-sharing of electronic signatures via training and policies is the responsibility of the customer.

---

(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.

Only administrators with appropriate rights may create new temporary passwords that grant users access to the Salesforce system. These passwords must be changed by their owners on first use, before they can receive access to Salesforce. All passwords are encrypted. Customers are responsible for training users on password secuirty and enforcing that passwords cannot be shared.

(b) ***Electronic signatures based upon biometrics*** *shall be designed to ensure that they cannot be used by anyone other than their genuine owners.*

As mentioned above, Salesforce does not directly support biometric devices such as fingerprint recognition and retinal scanning.

---

§ 11.300 Controls for identification codes / passwords.

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

(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.*

Salesforce maintains a unique login-name / password combination associated with every user granted system access. These combinations uniquely identify every user logging into the systems, so no two users can be granted access to the system under the same login name and password. User IDs can never be reassigned to another person.

All passwords within the Salesforce system are encrypted. Password length and complexity, such as the option to require both alphabetical and numeric characters, are system-configurable.

(b) ***Ensuring that identification code and password issuances are periodically checked****, recalled, or revised (e.g., to cover such events as password aging).*

All passwords must be changed immediately upon first use by their owner.

Password aging requires users to change their password after a specified period of time (system-configurable).

Password recycling is managed so that a user may not reuse a previous password for a specified amount of time (system-configurable).

(c) ***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.

Users may change their password anytime they believe that the integrity of the password has been violated. Administrators may revoke a user's access at any time or force the user to enter a new password at any time, when necessary to protect the integrity of the system. Customers should also have Standard Operating Procedures related to loss management procedures.

(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.*

All records of system access are maintained in the login history list within the Salesforce database. This information includes the user to whom access is being granted (username), login time of access, source IP address of the computer where access occurred, the login type for which access is being granted, the success of the login attempt, the browser program used for access to the application, the computer platform used for access, the application name, and the client version of the login application, along with the API type and version where the login is programmatically based.

All records of access violation are maintained in the Salesforce database and may be displayed online. The system administrator also has access to audit reports that logs all records of access violation. Additionally, customers can configure email notifications for all access violations.

(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.*

Salesforce.com periodically performs internal security assessments and also uses external service providers to perform an application vulnerability assessment after each major release. These assessments include tests on authentication infrastructure to ensure there are no vulnerabilities. Customers should also consider implementing best practices such as IP address restriction and two factor authentication.

BIBLIOGRAPHY

Federal Register/Vol. 62, No 54/Rules & Regulations/Part 11, Electronic Record; Electronic Signatures; Final Rule. www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf, March 1997.

The General Principles of Software Validation. FDA, 2002.

Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application. http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM072322.pdf, August 2003.

CONTRIBUTIONS AND PEER REVIEW

Finamore, Robert. qPharma.

Leibowitz, Marc. Salesforce.com.

Martin, Kevin. CQV.

Ott, Ryan. CQV.