

**Winchester Business Systems, Inc.'s
Interpretation of 21 CFR Part 11**

Electronic Records & Electronic Signatures

June 1, 2002

Table of Contents

Introduction

Part 11 Description

 Closed and Open Systems

 Controls for Closed Systems from Subpart B Sec. 11.10

 Closed Systems Compliance Requirements

 Electronic Signatures-- How are electronic signatures employed?

 Definitions

Winchester's Approach to

 Electronic Records

 Electronic Signatures

 Implementation of Winchester's Approach

 Winchester's Part 11 Compliance Product – ComPac GxP

 Winchester's Part 11 Compliance Services

Part 11 Defined and Winchester's Responses

 §11.10 Controls for Closed Systems

 §11.30 Controls for Open Systems

 §11.50 Signature Manifestations

 §11.70 Signature/Record Linking

 §11.100 General Requirements

 §11.200 Electronic Signature Components and Controls

 §11.300 Controls for Identification Codes/Passwords

Why Winchester?

References

Introduction

Documents may contain vital information about a sensitive subject. Often, these documents would identify who wrote the document and when the document was written. In a perfect world, the document would not require any changes after it was initially written.

In our world we must deal with real documents, electronic or otherwise every day. Our electronic documents tend to go through what some administrators describe as a very elaborate “life cycle.” Our electronic documents are authored, reviewed, edited, approved, published, and submitted. Sometimes the real purpose of an electronic document’s existence is to track events and changes as they occur.

In the real medical world, documents must truly identify every author, reviewer, approver, publisher, and administrator that has had something to do with the document – even if they merely made electronic comments about the content of a document. This requirement for authenticating people who author or change a document as well as record the changes to documents has given rise to some serious regulations as published by the US Food and Drug Administration.

Within the Code of Federal Regulations, (CFR), a recent addition was published numbered 21 CFR Part 11, (Part 11). Part 11 is titled:

Electronic Records; Electronic Signatures.

The purpose of this position paper is to summarize the requirements of Part 11 and to show how Winchester Business Systems, Inc. (Winchester) has developed and deployed products, practices, and services to address each of the Part 11 requirements.

Winchester provides further explanation of its products, practices, and services in response to your queries through e-mail (info@wbsnet.com), our web site at (<http://www.wbsnet.com>), and by telephone (1-888-749-7150 in the United States and 1-781-503-0200 internationally).

Part 11 Description

Part 11 sets forth the requirements for the creation, modification, maintenance, archival, retrieval, and transmittal of electronic records and also the use of electronic signatures when complying with the Federal Food, Drug and Cosmetic Act or any other Food and Drug Administration (FDA) regulation. These rulings became effective in March 1997. Part 11 was developed as a cooperative effort between the industry and the FDA.

Part 11 “provides criteria under which FDA will consider electronic records to be equivalent to paper records and electronic signatures equivalent to traditional handwritten signatures.” Part 11 states that records may be held in electronic form and electronic signatures may be used in lieu of “handwritten” signatures.

REGARDING RECORDS: Part 11 applies to any existing paper records requirements and “supersedes any existing paper record requirements by providing that electronic records may be used in lieu of paper records.”

REGARDING SIGNATURES: “Electronic signatures which meet the requirements of the rule will be considered to be equivalent to full handwritten signatures or initials.”

These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology compatible with FDA’s responsibility to promote and protect public health.

However, the use of electronic records by any organization as well as their submission to the FDA is voluntary.

In general, the controls noted in Part 11 are meant to:

1. Ensure rigorous conformance to the established computer systems validation methods that are crucial in the FDA regulated industries; and
2. Satisfy the FDA's requirements for archiving both the records themselves and the audit trail of all changes and accesses of a particular document throughout its "lifetime"

The *Benefits* to an organization for using Electronic Signatures are:

- ❑ Electronic environment
 - Procedures / Protocols
 - Clinical / Batch data
- ❑ Electronic communication
 - Internal
 - Agency
 - Contracted parties

The *Impact* on an organization for using Electronic Signature is:

- ❑ Reduced paper handling may mean reduced costs
 - Tighter and more reliable control over manufacturing procedures
 - Tighter and more reliable control over corrective actions
 - Better and more accessible trending data
- ❑ "Quick and easy" access to documentation along with lower risk of losing important documents!
- ❑ Faster document cycle times

According to the "Guidance" published by the FDA subsequent to the publication of Part 11, the FDA views systems in one of two fashions, Closed or Open.

Closed and Open Systems

CLOSED SYSTEMS: *Closed systems* are defined in the “Guidance” as "an environment in which system access is controlled by persons who are responsible for the content of electronic records that is on the system."

OPEN SYSTEMS: *Open systems* are defined as “an environment in which system access is not controlled by persons who are responsible for the content of electronic records that is on the system.”

Important FDA commentary:

- ❑ “...the most important factor in classifying a system as open or closed is whether the persons responsible for the content of the electronic records control access to the system...”
- ❑ “...The agency does not believe it is necessary to codify the basis or criteria for authorizing system access, such as the existence of a fiduciary responsibility or contractual relationship.”

Controls for Closed Systems from Subpart B Sec. 11.10 :

In general:

Organizations that 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.

Functional characteristics for a closed system include:

- ❑ Physical access control,
- ❑ Approved standard operating procedures around system operation, usage and maintenance,
- ❑ Employees and supervisors trained in the procedures,
- ❑ Investigations when abnormalities occur,
- ❑ Being under legal obligation to the organization responsible for operating the system.

Closed Systems Compliance Requirements:

1. The system must be validated.
2. The company must demonstrate the ability to generate accurate and complete copies of record in both human readable and electronic form
3. The company must demonstrate that records can be accurately and readily retrieved during the records retention period
4. Access to the system must be limited to authorized individuals
5. The system must use 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. (NOTE: the audit trail itself becomes an “electronic record” subject to requirements of Part 11)
6. The system must use operational system checks to enforce permitted sequencing of steps and events, as appropriate
7. The system must use 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
8. The company must demonstrate that the use of a device (e.g., terminal, personal computer, etc.) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
9. The company must be able to demonstrate that the persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
10. The company must demonstrate they employ written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification
11. The system must employ appropriate controls over systems documentation including:
 - ❑ Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
 - ❑ Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Electronic Signatures-- How are electronic signatures employed?
(21CFR11.50 - 11.70)

The electronic record must show:

- ❑ Signer's printed name
- ❑ Date/time of signing
- ❑ Meaning of signature (e.g.: review, approval)

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. (21CFR11.70)

These signatures are subject to all the controls mentioned for open/closed systems

Definitions

Handwritten signature -- 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 a document with a writing or marking instrument such as 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.

Digital signature -- an electronic signature based upon cryptographic methods.... such that the identity of the signer and the integrity of the data can be verified

Electronic record -- 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

Electronic signature -- 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.

Winchester's Approach to Implementation of Electronic Records and Electronic Signatures

Winchester has a unique, complementary approach to each subject -- Electronic Records and Electronic Signatures:

Winchester's Approach to Implementing Electronic Records

Winchester's approach is to develop an electronic record audit trail that captures the "value" or content of each desired or field to be tracked in a document. The audit trail is recorded in a document/record that is "separate" from the document being tracked.

Whenever a new document is initiated, an audit trail document is generated as well. The "document id" of the original document is captured to track all changes to the master document after it was initiated. Each time a document is "opened" in the "edit" mode, a snapshot is taken of the tracked fields and their respective values. When the document is "saved," a snapshot is taken again of the tracked fields, if any field has been changed, a message is written to the audit trail document describing the field name and both the "before" and "after" values. The user's id file is interrogated. The user's name and the date and time of the save event are written to the audit trail document.

Audit trail documents are not kept in the same accessible view and location as the master documents. They can be kept in an entirely separate database where the only access is "read only" to any authorized user. A "tab" can be inserted on the master document which would allow a user to "view the audit trail documents" in chronological order.

Features of Winchester's Approach to Electronic Records:

- ❑ Specific Forms and Document Types may be selected to generate audit trails
- ❑ Specific fields are selected or not-selected on a document/form to be tracked
- ❑ Audit trail documents cannot be edited, changed, or deleted
- ❑ Audit trail documents contain the before and after values of any field that was altered during a specific edit session
- ❑ Audit trails contain the unique, operating system-issued document id of the master documents being tracked
- ❑ Audit trails contain the name of the user that made the change as well as the date and time the change was saved by the user.
- ❑ One of the fields on the audit trail can contain the profile id or "electronic signature" of the person that made the change.
- ❑ Users can not turn on or off audit trails. They are a natural part of the specific application.

Winchester's Approach to Implementing Electronic Signatures

Winchester's approach to developing an electronic signature is built upon the realization that passwords that have been issued by any company's Information Technology administration may not be considered suitable to prove the identity of a user. Based upon that premise, Winchester has developed a password and electronic signature approach that is unique to each and every application or database.

1. **Check for Access** --When a user opens an application for the very first time, the Access Control List (ACL) is checked to determine what level of access that the user may have. They must have at least "Reader Access" to open the application. If the default access is "No Access" and the user's name is not contained in the ACL as at least having "Reader Access", **access is denied** to the user. The user's name need not be contained in the ACL if they are listed in the company's Name and Address Book (NAB) as a member of a group that does have access and that group is listed in the ACL.
2. **If Access is Denied** -- If the new user is allowed access, the application immediately interrogates the user for a new "profile" password that will be recorded within the application. That password will be required to create/compose a new document or edit an existing document – assuming the user is listed as having at least "Author" access to the database within the ACL.
3. **If the User can Create or Edit a Document** -- If Author or Edit access is permitted to the user, the user is queried for his application-specific password at the end of the session when he tries to "save" the document he has either created or edited. The password that is entered is authenticated against the password that the user originally entered. If the authentication fails, the user is informed of the failure and the document is left in its "open" state without saving it. The user may attempt to save the document again but they must supply the correct profile password.

Design Considerations -- Application-specific passwords can be forced to have specific characteristics. For instance, they can be required to be in excess of a certain number of characters. The National Security Agency (NSA) suggests that the lower limit to password length be eleven characters. The industry suggests that to ensure proper password content the password contain both upper- and lower-case characters as well as special characters like periods, commas, question marks, etc. Winchester's approach can be made to require the adherence to these specifications. The user would be forced to comply with the size and type of password at his initial session.

Features of Winchester's approach to Electronic Signatures:

- ❑ A special field exists on the actual document being created/saved that contains the electronic signature (bit configuration taken from the user's id) of the last person that saved the document
- ❑ The profile password that is used for the application is unique to the application. The application password is different to the user's login password to Notes and to the user's Network.
- ❑ Winchester's Approach to application password is completely web-compatible.
- ❑ The password configuration can be determined as a matter of client-company policy and can meet both FDA and NSA suggested formats.
- ❑ Documents that are created or composed or edited and saved within the application require that a correct profile password be entered by the user.
- ❑ Winchester's Electronic Signature approach can be a component of Winchester's Electronic Record approach.
- ❑ Profile passwords expire and must be updated by the user according to the organization's policies.

Implementation of Winchester's Approach to Electronic Records and Electronic Signatures

As Winchester has written and tested the coding for both Electronic Signatures and Electronic Records of live databases, much of the development effort has been born previously as a Winchester-internal project.

Winchester has developed both products and services for its clients to assist them in becoming compliant with Part 11.

Winchester's Part 11 Compliance Product – ComPac GxP

Winchester has developed many computer software products that are in compliance with Part 11, right from their inception. Winchester has placed the proper compliance directives directly into the program code of Winchester's products.

As part of Winchester's expanding product plan, Winchester has developed a self-contained module that can be "bolted on" to an application such that the application can become compliant with Part 11. Winchester's Compliance Package product is named "ComPac GxP."

ComPac GxP was developed exclusively for regulated companies, especially those governed by FDA-regulations. The system was specifically designed to help these organizations achieve Part 11 compliance. ComPac GxP does not require the expenditure of additional technology investments in that it leverages existing technology already in production at most pharmaceutical, medical device, and biotechnology firms while providing an enhanced level of security and built-in business rules and best practices to help organizations achieve compliance.

ComPac GxP is a modular component of every application product developed and supplied by Winchester. This use of ComPac GxP ensures integrity, commonality of design, and consistency of application for all Winchester products.

Winchester offers the ComPac GxP product to qualified clients for their development staffs to use to upgrade legacy applications as well as design new applications to become compliant with Part 11.

Winchester's Part 11 Compliance Services

Winchester provides industry-focused, management consulting and information technology consulting services to:

- ❑ Improve business processes
- ❑ Design and deploy computer applications that are Part 11 compliant
- ❑ Validate systems and their operating environment for Part 11 compliance
- ❑ Assess current and planned systems for Part 11 compliance
- ❑ Develop SOPs for Part 11-related business processes
- ❑ Author the plan for an organization to achieve Part 11 compliance

Improve Business Processes – The advent of a new system to manage documents electronically, assist with the project management of a clinical trial, track adverse events, manage queries from the FDA, and other new systems provides an opportunity to improve the associate business processes. Winchester has developed and proven techniques to optimize manual processes in support of automated systems.

Design and Deploy Computer Applications that are Part 11 Compliant --Winchester's services to develop specific applications in the regulatory environment are unsurpassed. Some of the systems that Winchester has developed for clients in the medical/regulatory industry have been used to save millions of dollars, automate business processes, improve safety environments, and help formulate better relationships between Winchester's clients and their customers and other business partners.

Validate Systems and their Operating Environments – Winchester's software validation specialists have experience providing professional levels of validation service in the regulated environments of biotechnology, pharmaceutical, and medical device companies. Winchester's Validation services encompass the entire spectrum of Software Quality Assurance. Winchester's Validation Services focus on the issues pertaining to systems and software for the pharmaceutical, biotechnology, and medical device industries, with the goal of meeting regulatory compliance requirements for submissions.

Assess Current and Planned Systems for Part 11 Compliance -- Winchester has developed a methodology and a doctrine that assists Winchester's clients in becoming compliant with Part 11. Tasks begin with taking inventory and gathering facts about the present environment and systems. Appropriate assessments of coverage and risks are accomplished next followed directly by a Gap analysis. Once the Gap analysis is complete, the client and Winchester team develop a plan for (1) mitigation of the procedural controls that may be corrected for the short term, (2) remediation resulting in a long-term plan for improvement, and (3) maintenance of the now-compliant environment.

Develop SOPs for Part 11-related Business Processes -- Standard Operating Procedures describe the company's policies and guidelines whereby the company will conduct its business in a regulated environment. Policies are accompanied by the requisite operating procedures and user manuals that describe the individual tasks for performing functions in accordance with installed systems.

Author the plan for an organization to achieve Part 11 compliance -- Similar to the service described above, Winchester professional consultants work with client management to develop the plan whereby the client company will become compliant with Part 11 and remain compliant.

The remainder of this document presents the requirements set forth in Part 11, along with Winchester's interpretation of the requirements, and the solution provided by Winchester's products.

§11.10 Controls for Closed Systems
§11.30 Controls for Open Systems
§11.50 Signature Manifestations
§11.70 Signature/Record Linking
§11.100 General Requirements
§11.200 Electronic Signature Components and Controls
§11.300 Controls for Identification Codes/Passwords
References

§11.10 Controls for Closed Systems

§11.10 Ensure authenticity, integrity, and when appropriate confidentiality of electronic records.

- ComPac GxP provides for an enhanced application administration feature that allows application administrators to define permissions on each form, view, and document within the system. The permission capability within ComPac GxP is multi-leveled, defines user roles, and is comprehensive.
- Authenticity, integrity, and confidentiality of all electronic records within the ComPac GxP system are governed by a comprehensive set of permission levels that restrict access when appropriate.

§11.10 Minimize possibility of repudiation by signer

- Administrative users within the ComPac GxP module are granted the highest level of security and are able to restrict access to documents and specific applications in accordance with the organization's business rules. All actions taken against any control documents are recorded in secure audit trail.
- Each user upon login for the first time is required to establish his or her authentication credentials. This identifies each user's unique ID and password combination to the ComPac GxP system. Once established, these credentials are encrypted and applied to that user only. The ID and password required for logon is the Lotus Notes user name and password.
- ComPac GxP requires each user to have a second "profile" ID and password combination that enables him or her to authenticate or sign any document, change request, or process requested by the ComPac GxP.
- With the added security of the unique profile ID and password combination within the ComPac GxP system, repudiation of any signatory is minimized.

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

§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 agency.

- ❑ Each client organization is responsible for a program's suitability as used in the regulatory environment.
- ❑ Winchester assists its clients with the validation process by providing documentation and records during the installation and training services.
- ❑ ComPac GxP is supplied with a comprehensive validation protocol to assist the organization with planning and conducting the validation tasks and the deployment of ComPac GxP.
- ❑ ComPac GxP records any changes or modifications to any documents and places these events within the audit trail.
- ❑ Winchester's applications utilize native application to view and print stored documents. Winchester's applications contain views and on-line reports that can be printed or viewed in popular report generation systems such as Crystal Reports and Excel.
- ❑ Existing reports can be edited and additional reports can be created in the application itself or in Excel and Crystal Reports. These new reports can be added to the system by the end user. All previewed reports may be exported to an electronic format for dissemination.
- ❑ ComPac GxP and all Winchester applications permit the establishment of attributes for each controlled or uncontrolled document. These attributes are used for full-text searching and retrieval within the system.
- ❑ Winchester applications include a comprehensive set of reports that enable the production of any record in human readable form.
- ❑ Winchester applications also support most current desktop applications that run in a Windows or Macintosh environment.
- ❑ Support of multiple document formats provides the ability to generate accurate complete records in human readable and elec-

tronic form.

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

§11.10(d) Limiting system access to authorized individuals.

§11.10(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period of at least as long as that required for the subject electronic records and shall be available for agency review and copying.

- Winchester provides to its clients a description of minimum system requirements to ensure proper functioning of the Winchester applications. It is the responsibility of the user to develop and implement an appropriate back-up protocol and security measures to ensure records are protected.
- Winchester's applications and ComPac GxP include a detailed security system to protect all electronic records within the system. This security system also provides ready access and retrieval tool records within the Winchester applications.
- Winchester's applications are closed systems.
- All Winchester applications and modules have multiple levels of security.
- Winchester's applications allow system administrators to restrict access to applications and documents according to stated business rules and guidelines
- All changes to data made within each Winchester module is stamped with the name of the originator and the time and date of the change. Each change creates an individual entry and audit trail; therefore, previously recorded change information is retained. The data can be maintained indefinitely and can be tracked via the Winchester Audit Trail module within ComPac GxP. Data can be easily viewed or output in a HTML format.
- The ComPac GxP system audits all events and provides a detailed audit trail summary upon demand. The audit trail report is accessible only to administrative users. The audit trail includes computer-generated date and time stamps.
- Audit trail information can never be overwritten within the system.

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

§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.

- Winchester modules are structured such that actions can only be performed in the appropriate sequence. Required steps, such as approval routing, cannot be skipped.
- Winchester's workflow is "flexible" in the choices of the next step in a process.
- Pre-structured or pre-defined workflow sequences cannot be executed out of sequence.
- Winchester's workflow deployments are "date sensitive" and built-in actions and agents "complain" to administrators when timing requirements are not adhered to.
- Step sequencing is enforced throughout the ComPac GxP system.
- Winchester's applications are closed systems. All Winchester applications have multiple levels of security.
 - The first level of security limits access to the application itself.
 - The other levels of security limit access to menu options and roles for functions and reports within the system.
- User rights that are assigned on a role basis accomplish second level of objectives.
- Access to individual documents in Winchester applications as well as individual reports in all applications are controlled by security within the application that is based on a Notes user ID and membership in predefined access groups.
- ComPac GxP authenticates with Lotus Notes/ Domino for access by all users. Once in the Winchester application system, access and privileges are governed by the ComPac GxP security.
- ComPac GxP enables a system administrator to expunge or deactivate a user within the system. This does not delete the account but saves the account for the purpose of the audit trail. An expunged user no longer has any privileges within the system.

§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.

§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.

§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.

- ComPac GxP's Audit Trail provides a mechanism for verifying the specific physical location where a user was logged on when records were created or modified.
- Winchester's clients are responsible for developing policies regarding training.
- Winchester's Training System application when used in conjunction with other Winchester applications provides additional access control to operations based on employee certifications as well as tracking all training activities internal and external.
- Winchester applications track training against any control document for all users within the system.
- Winchester's clients establish a training program and develop operating procedures that govern classroom training.
- Classroom training is tracked within Winchester's Training system.
- Winchester's clients develop policies and procedures governing accountability.
- Winchester applications protect against falsification of records by creating audit trails that can be tracked via the ComPac GxP Audit Trail module.

§11.10(k)(1) Use of appropriate controls over systems documentation including:

Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

§11.10(k)(2) Use of appropriate controls over systems documentation including:

Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation

- Winchester's clients develop policies regarding controlled access to system manuals and system related documentation.
- Winchester's applications and the ComPac GxP system are closed, controlled systems requiring access privileges for entry.
- Winchester's clients develop policies regarding controlled access to system manuals and system related documentation.
- Documentation provided by Winchester is revision controlled.
- ComPac GxP includes a comprehensive change control methodology that requires a change request to modify any document.
- Any changes to any document are traceable through the audit trail.

§11.30 Controls for Open Systems

§11.30 Implement document encryption for record confidentiality (as appropriate)

- All Notes and profile ID and password combinations are encrypted for the protection of the user.
- Winchester's applications, including ComPac GxP, are controlled, limited access systems by definition.
- Document encryption is not mandatory for compliance with 21 CFR Part 11. However, all content is protected on the server using the 32-bit file ID so that the name of any content is not exposed outside of the ComPac GxP environment. These documents and files are hidden on the ComPac GxP server using Lotus Notes security.

§11.30 Use digital signatures for a record authenticity and integrity

- ComPac GxP is delivered with a default profile user ID and password authentication system. The system was designed to be flexible to allow digital signatures.

§11.30 Signature Manifestations

§11.50(a) Signed electronic records must contain: name, date/time of signing, and meaning of signature

§11.50(a)(1) Signed electronic records shall contain information associated with the signing that clearly indicates all 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.

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

- All electronic records within ComPac GxP include as protected attributes the name, date/time of signing, and meaning of signature.
- The meaning of signature is defined within ComPac GxP as a role.
- Users may have various roles depending on the nature of their signing. Rules regarding roles are established by the system administrator and tracked for each user.
- Each electronic record is stamped with the name of the individual carrying out a signed activity, and the time and date that the signature was applied to the electronic record.
- The meaning of each signature is automatically indicated with the signed record.

- All Winchester modules contain reports that can be printed or viewed in the application or in popular report generating products like Excel and Crystal Reports.
- Existing reports can be edited and additional reports can be created in the application or in the report generator and added to the system by the end user.

§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.

- Winchester applications are secure systems. There are no means to remove or copy signatures from/to documents by ordinary means.
- ComPac GxP includes an irrefutable link between the electronic record and the electronic signatures. Once an electronic signature has been applied to a document, the object is frozen and the signature object and document are irrefutably linked.

§11.100 General Requirements

§11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

- Winchester applications and ComPac GxP have a profile user ID and password authentication protocol that will not allow the entry of duplicate active records. The control of reuse and reassignment of user IDs and passwords is beyond the scope of Winchester's applications. It is the responsibility of the user to establish user ID and password assignment policies and procedures.
- ComPac GxP is delivered with a profile user ID and password combination authentication system. The system enforces the uniqueness of this profile user ID and password combination for authentication.

§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.

- This activity is beyond the scope of Winchester applications. It is the responsibility of Winchester's clients to establish hiring policies and procedures to verify the identity of the individuals hired.
- Winchester's applications include a report describing activities by each user. The user activity report summarizes each user within the system with an established electronic signature.
- The user activity report can be presented to regulatory authorities as verification of the identity of individuals receiving electronic signature.
- The user activity report includes the users name, Job Title, Winchester's profile ID, and the profile users ID in the underlying Winchester application. It will also indicate if the user is an administrative user, list of groups they are in, and if the user is expunged (inactive) or not.

§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.

§11.100(c)(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

§11.100(c)(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.

□ Each organization is required to notify the FDA in writing of its intention to use electronic signatures. It is the responsibility of Winchester's clients to perform this notification.

□ This is processed by each individual client organization and is beyond the scope of Winchester's applications and ComPac GxP.

□ This is processed by each individual client organization and is beyond the scope of Winchester's applications and ComPac GxP.

§11.200 Electronic Signature Components & Controls

§11.200(a)(1) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.

§11.200(a)(1)(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 will be executed using at least one electronic signature component.

§11.200(a)(1)(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.

§11.200(a)(2) Electronic signatures that are not based upon biometrics shall: Be used only by their genuine owners; and

§11.200(a)(3) Electronic signatures that are not based upon biometrics shall: 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.

- Winchester employs a non-biometric signature model with a combination of a user ID and password for identification at sign on and a second ID and password at document saving and signing.
- The user ID and password are double authenticated for every sign-off via the Winchester password authentication and the profile secondary password authentication.
- The user ID and password and profile ID and password are encrypted upon entry such that no part of the user's non-biometric signature is exposed at any time.
- ComPac GxP uses all authentication components for each signing in a continuous session.
- Same as above
- The user ID and password combination within ComPac GxP is established for the sole use of the genuine owner. Corporate policy governs the protection of the user ID and password combination.
- The user ID and password combination are encrypted upon entry by the user. To gain access to another users ID and password, requires the collaboration of the original owner and the unauthorized user.
- ComPac GxP is fully compliant with this section of the regulation.

§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.

- Winchester applications do not utilize signatures based on biometrics.
- ComPac GxP is designed with the flexibility to use biometric or nonbiometric electronic signatures.
- ComPac P GxP does not directly control biometric signatures but provides security against the unauthorized attempted use of a biometric signature

§11.300 Controls for Identification Codes/Passwords

§11.300(a) 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:

(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.

§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).

- Winchester has a user ID and password authentication protocol that will not allow the entry of duplicate active records
- The rules governing the ID and password combination are as follows:
 - The ID and profile password are defined as the electronic signature for the user
 - No user in the system can have exactly the same combination of authentication details. If such a combination already exists, the user receives an error message. This rule applies regardless of whether a previously used combination was that of the user or another person.
 - The ID and profile password are case sensitive.
- Since Winchester security system is tightly integrated with Lotus Notes Security, all of the security policies identified within Lotus Notes are automatically inherited by Winchester to provide compliance to Part 11 requirements.
- Passwords within ComPac GxP are reviewed at creation time by system agents to verify uniqueness. Internal operating procedures specific to each client location shall govern the frequency of ID and password verification. Only the authorized user has the ability to change his/her ID/password nonbiometric electronic signature credentials.

§11.300(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.

§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.

- Through its audit trail, ComPac GxP tracks any modification of a user's authentication details. The date and time of modification are shown in the audit trail report.
- Other parts of this subsection are not applicable to Winchester as there are no devices that bear or generate identification code or password information.
- Since Winchester's security system is tightly integrated with Lotus Notes Security, all of the security policies identified within Lotus Notes are automatically inherited by Winchester to provide compliance to Part 11 requirements.
- Upon any unauthorized entry attempt, a message box is displayed to the user that states, "cannot authenticate. Authentication failed. Supplied authentication ID or password is incorrect."
- The unauthorized attempt information is captured in the audit trail with a date and a time stamp.
- Optionally, ComPac GxP can provide a time-out security check. This feature of Lotus Notes times out by default after "n" minutes of mouse or keyboard inactivity. The user is forced to reapply their password to reopen the session. Time-outs prevent unauthorized walk up attempts to search within the system if a user steps away from his or her workstation with an open active session.

§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.

In Winchester's clients, device testing is governed by the client's standard procedures. Testing is beyond the scope of ComPac GxP and Winchester's applications.

Why Winchester?

Winchester has significant experience developing and deploying systems and procedures that meet the needs of a growing and successful company that is concerned about electronic records and electronic signatures. An engagement team from Winchester has many years of directly related experience.

Winchester has a technology base of experienced consultants for helping clients plan, manage, and deploy groupware applications in a regulatory environment. Winchester has specific experience in large-scale rollouts of Lotus Notes, both in client settings and internally as part of Winchester's own internal deployment. Winchester has access to additional technical resources with detailed knowledge of the architecture, capabilities and future evolution of the Lotus Notes product. Winchester is uniquely qualified and positioned to help our clients integrate Lotus Notes into their overall Information Architecture.

Winchester has:

- ▣ An application template already developed that can be used to assist a client with achieving compliance with Part 11 that fulfills the client's needs for electronic records and electronic signatures;
- ▣ Direct, related experience in FDA-regulated industries as well as hands-on experience developing and deploying Lotus Notes-based systems to satisfy similar requirements;
- ▣ Joint Application Development (JAD) sessions where Winchester developers and client personnel can work hand-in-hand on projects; and
- ▣ Consulting services that concentrate on improving client infrastructures and processes.

Due to the comprehensive nature of Part 11 and the impact it has on existing systems, many organizations have struggled to understand and interpret the ruling as it applies to their systems. Further, many existing client systems were not originally developed with considerations for Part 11. Winchester can help a client achieve the success with Part 11.

References

1. Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures Validation, August 2001 -- Draft
2. Electronic Records: Electronic Signature Certification; FDA Office of Regulatory Affairs, Field Management Directive No. 146; August 20, 1997 – Original
3. Legal Considerations in Designing and Implementing Electronic Processes; A Guide for Federal Agencies; Department of Justice; November 2000 – Original
4. Records Management Guidance for Agencies Implementing Electronic Signature Technologies; National Archives and Records Administration, October 18, 2000 – Original
5. Guidance for Industry, Computerized Systems Used in Clinical Trials; FDA; April 1999 – Original
6. Electronic Records; Electronic Signatures; Final Rule; 21 CFR Part 11; FDA; March 20, 1997 – Final Rule
7. Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures Time Stamps, February 2002 -- Draft
8. General Principles of Software Validation; Final Guidance for Industry and FDA Staff; FDA; January 11, 2002 – Final
9. Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures Glossary of Terms, August 2001 -- Draft
10. Security Self-Assessment Guide for Information Technology Systems; National Institute of Standards and Technology; NIST Number 800-26; August 2001
11. Guidance for Industry, Providing Electronic Submissions in Electronic Format; FDA; January 1999 – General Considerations