

RAPID-Pharma™ AND 21 CFR PART 11

Automsoft®

INTRODUCTION

In 1997 the US Food and Drug Administration introduced the 21 CFR Part 11 regulations on "Electronic Records and Electronic Signatures" (hereafter Part 11 for brevity). This regulation is applicable to software used in the manufacturing of pharmaceuticals, medical devices and in bio-tech products. The Part 11 regulation is, in part, intended to ensure that whenever manufacturers replace paper based records with electronic records (i.e. software) that they are (legally) equivalent to those paper based systems they are replacing.

In February 2003, the FDA announced that they were withdrawing all of the draft guidance for industry documents, and instead issued a new guidance document – "Part 11, Electronic Records; Electronic Signatures – Scope and Application". This draft outlines a more pragmatic approach to the enforcement of Part 11 based on the FDA's new risk based approach to computer systems. Contrary, to what some observers believe, Part 11 has not been diluted, instead the FDA is applying a common sense approach to management of electronic records and signatures. And, of course, the business benefits of deploying Part 11 software- such as RAPID-Pharma – still apply, for example less or no paper to sign, print, manage and submit.

The purpose of this white paper is to explain how RAPID-Pharma completely addresses the Part 11 regulation. In particular, the types of record stored in RAPID-Pharma are identified along with an explanation of RAPID-Pharma's support for key Part 11 requirements. These are:

- : Security (and authentication)
- : Electronic signatures
- : Audit trail

Automsoft is committed to developing software which responds to the changing requirements of the FDA regulated industries. This white paper will help end users and decision makers to see how modern software products, such as RAPID-Pharma, can respond to such regulations, and help reduce the ongoing support and validation costs for such systems.

WHAT IS RAPID-PHARMA?

Automsoft's RAPID technology is a suite of advanced database software designed specifically for process industries. RAPID offers the highest level of performance in the marketplace today, providing manufacturers with the ability to view online the status of the production process, in addition to the complete historical record of the manufactured product. RAPID allows manufacturers to collect, store and report on production data in a secure environment.

RAPID-Pharma is a pre-configured extension of the RAPID product suite that has been specifically designed for the pharmaceutical and bio-tech industries. RAPID-Pharma adds extra functionality to satisfy the regulatory needs – Part 11 – of these industries. These include, but are not limited to, integrated security, digital signature capabilities and a comprehensive audit trail.

Note: RAPID-Pharma is a Commercial off the Shelf (COTS) software product. It is built on client/server technologies and runs on the Microsoft Windows family of operating systems.

THE IMPLEMENTATION OF PART 11 IN RAPID-Pharma™

PART 11 SUPPORT

Part 11 divides the controls that must be in place into two categories - procedural and technical. Technical controls are within the scope of a software product (if deployed correctly), procedural controls are not. These procedural controls should be addressed by the end users organization with Standard Operating Procedures (SOPs).

In addition, it will be assumed for this white paper that RAPID-Pharma will be used in 'closed' system. RAPID-Pharma may be deployed as an 'open' system in which case the additional technical (and procedural) controls will be provided by the end users organization.

Table 1 details how RAPID-Pharma meets the requirements of the regulation. It also provides a point by point description of those controls which must be handled by an SOP.

RAPID PHARMA DEFINITIONS

RAPID-Pharma Electronic Records

Part 11 has a very broad definition of what constitutes an electronic record, although this has been narrowed somewhat in the draft guidance document. To clarify electronic records in a RAPID-Pharma context, we can divide them into electronic record classes; these include:

- : Data collected automatically without human intervention (raw process data)
- : The system configuration (meta-data)
- : Reports (PDF documents) and other binary data
- : Audit records (in the Audit Trail)

Electronic Signature

Part 11 clearly defines what constitutes an electronic signature, but does not differentiate between using the signature elements for different purposes. RAPID-Pharma uses the users Windows credentials to both identify the user and, to effect an electronic (digital) signature. Note that, if the intention of the use of the users Windows credentials is to identify that user e.g. changing an item dead band, for audit trail purposes, then that is not an electronic signature.

RAPID-PHARMA'S IMPLEMENTATION OF THE KEY COMPONENTS OF PART 11

This section details how RAPID-Pharma implements Security, Electronic Signatures, and the Audit Trail.

SECURITY

RAPID-Pharma leverages the Windows NT/2000/XP security sub-systems to satisfy Part 11 security (and electronic signature – see below) requirements. Using the security system provided by the operating system yields a number of important benefits including:

- : Users (and groups) need only be configured once i.e. with the Windows User Manager for Domains or Active Server
- : RAPID-Pharma does not need to store either user names or passwords
- : Windows security settings are automatically picked up by RAPID-Pharma such as password aging, retry attempts, etc.

Permissions and Privileges

In common with the Windows security model, as installed the RAPID-Pharma system is unsecured. The RAPID-Pharma system administrator may then apply security settings to databases, templates and reports. Security settings (permissions and privileges) are administered through the Configuration Tool. The following are the RAPID-Pharma specific permissions:

- : Read – Allow read only access to a resource
- : Write (create/update) - Allow creation and changes to resources
- : Delete – Allow resources to be deleted
- : Change Permissions – Allow permissions for a resource to be changed

There is one RAPID-Pharma privilege defined:

- : Take Ownership – as per the Windows privilege Take Ownership.

A user with the Take Ownership privilege can "own" a resource. This privilege is by default usually only granted to Windows system administrators. The granularity of these permissions and privilege is at the database level for databases, and at all levels for templates and reports e.g. folder or individual file. Permissions may be set on a per user basis or more commonly on a per group basis.

Note that, in practice, security is very easy to administer - system administrators can create a RAPID-Pharma group, assign access permissions to that group, and add/remove users from the group as required. You do not need to be a full time system administrator.

Authentication

RAPID-Pharma users are identified to the system by their Windows credentials (domain user name and password pair) and Groups membership to determine access permissions. If security is enabled then users are prompted for their Windows credentials for authentication purposes. RAPID-Pharma then asks the domain controller to authenticate the credentials. If the credentials fail to authenticate then an audit record is generated indicating the failed attempt. If the credentials authenticate then RAPID-Pharma will check the user's privilege level for that resource and either allow or deny the action.

If after a (configurable) timeout period of inactivity has expired the user will be prompted for the password component of their credentials, and the checks above repeated. This prevents misuse of the user's credentials by another person either deliberately or accidentally.

¹ More accurately, it's associated with the users Windows SID rather than their credentials. The SID is invariant to password aging etc.

ELECTRONIC SIGNATURES

As noted above, RAPID-Pharma employs the users Windows credentials to effect an electronic signature on a report (document). Adobe Acrobat® technology is used to both convert the on screen report into a PDF document and to generate a digital signature for inclusion in the document, based on the supplied credentials.

Self-Sign

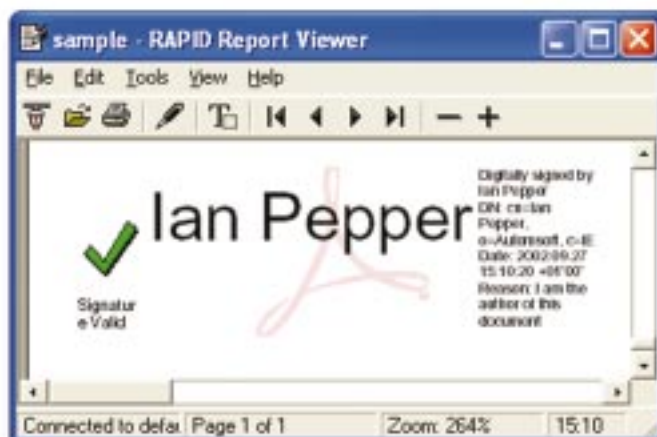
RAPID-Pharma uses the Adobe Self-Sign feature to generate the PKI based signature. The complexity of generating the certificate portion of the signature is hidden from the user- it is generated automatically the first time a user signs a report. The certificate is stored in the RAPID-Pharma database, and is associated with those the users credentials , for further signings. The certificates may also be exported from the RAPID-Pharma database for use outside of this system.

Signature Manifestation

The visible form of the digital signature includes:

- : The signer's full name
- : The date and time of signing (in local time)
- : The reason for signing

The reason may be selected from a drop down list of common reasons e.g. "I am approving this document", "I am the author of this document", or may be entered in free text at the time of the signing.



If the signature is validated then it has a green tick mark before it, if it has not been validated then it has a yellow question mark before it, finally if the signature is invalid then it has a red 'X' before it.

AUDIT TRAIL

Part 11 requires that a comprehensive audit trail of every human interaction with the systems electronic records is provided. However, there is also an implicit requirement for some method of viewing and searching the audit trail i.e. a reporting tool. RAPID-Pharma includes a complete unobtrusive audit trail database component and a flexible audit reporting tool.

Audit Database

The audit trail is stored in a discrete Audit Database, which can reside remotely from the RAPID-Pharma system database(s) i.e. data. The audit database is linked to the RAPID-Pharma system databases through the RAPID-Pharma software itself. Placing the audit trail in a discrete database was a conscious design decision, as opposed to using any built in audit trail capability that comes as standard with many RDBMS. The RAPID-Pharma approach has a number of distinct advantages, for example:

- : It supports multiple RAPID-Pharma installations — so you can audit the whole enterprise in a single unified audit trail
- : The audit database may be centrally located away from the process data
- : The audit database may be hosted on another computer and is therefore easily (physically) secured

In the deployment model where the audit database is hosted on a central computer, should the network fail for any reason then the RAPID-Pharma system database will cache audit records locally. This behavior is automatic and continues until such time as the failure has been rectified. In the background, RAPID-Pharma checks for network availability – once established the locally cached audit records are sent to the audit database proper and the local cache deleted.

The Audit Database is self-auditing — so that the audit records themselves adhere to Part 11 conventions. For example, if audit records are deleted from the audit trail by the RAPID-Pharma system administrator (providing the administrator has delete privileges) then an audit record is written back into the audit database indicating that a delete operation has occurred. A log file is also generated which contains the deleted audit records in XML format.

Audit Records

Part 11 requires that the audit record includes the local time of the action, the full name of the person who performed it and the reason for the change. RAPID-Pharma's Audit Database stores this information and much more including:

- : The time the action occurred (in both local time and UTC)
- : The type of action performed e.g. Update, Create, etc.
- : The full name of the user who performed the action (from the Windows security system)
- : User details such as job title and domain name (from the Windows security system)
- : The module or tool used and its Process ID (PID)
- : Before/after states of the record affected (where applicable)
- : The explanation or reason for the action (as free text)

The Audit Database stores the original values of any altered or deleted records. Audit database records are rendered into a human readable format through the Audit Reporting Tool.

Audit Reporting Tool

To satisfy Part 11, Audit Database records must be easily accessible in human-readable form. The Audit Database may be queried with RAPID-Pharma's Audit Reporting Tool. This query tool is web based and must be hosted on a web server which supports ASP e.g. Internet Information Server. The Audit Reporting Tool renders the XML retrieved from the audit database into human readable HTML for display in a web browser.

The Audit Reporting Tool can query the audit database under the following parameters:

- : The RAPID-Pharma database name
- : The Audit Database itself
- : User name
- : Time of action
- : Type of object affected (e.g. Item, Phase, Route, Folders & Objects)
- : The action performed (e.g. Create, Update, Failed Access)
- : Tool or module involved (e.g. Excel Add-in, Configuration Tool)
- : All of the above

PART 11 AND RAPID-Pharma™

Table 1 describes how RAPID-Pharma meets the requirements of the regulation. It also provides a description of those controls that must be handled by an SOP.

TABLE 1

Regulation section

Regulation text

RAPID-Pharma Solution

B-11.10.a

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

Automsoft supply a generic IQ document to assist in validation but the overall validation exercise remains the customer's responsibility.

B-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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

All reports, process data and meta data are stored in the RAPID- Pharma Database. Data may be exported in multiple formats including XML, CSV, PDF, etc. and is accessible both by tools provided by Automsoft and through third party products.

B-11.10.c

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

User rights, to both the database and report templates, are strictly controlled. Any attempt to change a record will be audited in the audit trail.

B-11.10.d

Limiting system access to authorized individuals.

System access is granted by the RAPID-Pharma System Administrator using RAPD-Pharma's security features.

B-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 at least as long as that required for the subject electronic records and shall be available for agency review and copying.

RAPID-Pharma uses a separate database to store the audit trail. The audit trail contains user's name, time and date (in both local and UTC formats), change details (including what was changed, where and how), value before and after the change. All this information is stored with the same level of security as the RAPID-Pharma database. The database is queried to produce the desired detail on a change and the information can be queried and sorted in a variety of ways including by operator name, batch ID, time and date, change type, etc.

B-11.10.f

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

Plant data is acquired on an event basis. When the data changes it is logged. There is no sequencing control involved.

TABLE 1 (continued)
Regulation section

Regulation text

RAPID-Pharma Solution

B-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.	Customers can configure RAPID-Pharma to require username and password checking for all levels of user.
B-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.	RAPID-Pharma restricts access to the database and configuration tools to those who have the appropriate security privileges only.
B-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.	This requirement is the responsibility of the customer and should be handled with an SOP.
B-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.	This requirement is the responsibility of the customer and should be handled with an SOP.
B-11.10.k	Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time sequenced development and modification of systems documentation.	This requirement is the responsibility of the customer and should be handled with an SOP.
B-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.	This requirement is the responsibility of the customer and should be handled with an SOP.

TABLE 1 (continued)
Regulation section

Regulation text

RAPID-Pharma Solution

B-11.50 a	<p>Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</p> <p>(a)(1) The printed name of the signer</p> <p>(a)(2) The date and time when the signature was Executed</p> <p>(a)(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature</p>	<p>The printed name of the signer is clearly displayed.</p> <p>The date and time the signature is executed is clearly displayed.</p> <p>The user is prompted for the meaning of the signature and the meaning is clearly associated with the signature (the reason).</p>
B-11.50.b	<p>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).</p>	<p>The items identified in paragraphs (a)(1), (a)(2), and (a)(3) are stored in the RAPID-Pharma Audit database and are subject to the same high integrity and security as all data records.</p>
B-11.70	<p>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.</p>	<p>Electronic signatures are linked to their respective records through the RAPID-Pharma software. All data held in the RAPID-Pharma database is held securely and cannot be tampered with.</p>
C-11.100.a	<p>Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</p>	<p>This requirement is the responsibility of the customer and should be handled with an SOP.</p>
C-11.100.b	<p>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.</p>	<p>This requirement is the responsibility of the customer and should be handled with an SOP.</p>
C-11.100.c	<p>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.</p> <p>(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.</p> <p>(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.</p>	<p>This requirement is the responsibility of the customer and should be handled with an SOP.</p> <p>This requirement is the responsibility of the customer and should be handled with an SOP.</p> <p>This requirement is the responsibility of the customer and should be handled with an SOP.</p>

TABLE 1 (continued)
Regulation section

Regulation text

RAPID-Pharma Solution

C-11.200.a

Electronic signatures that are not based upon biometrics shall:

- (1) Employ at least two distinct identification components such as an identification code and password.
 - (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 shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.
 - (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.
- (2) Be used only by their genuine owners
- (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.
 - (3)(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

RAPID-Pharma employs the users Windows username and password.

RAPID-Pharma utilizes a username and password to execute a signing, and password only for subsequent signings which are performed as part of a single continuous session.

RAPID-Pharma can be configured to automatically log-off a user after a period of inactivity. Once an automatic log-off has occurred a user must subsequently re-enter both the username and password.

This requirement is the responsibility of the customer and should be handled with an SOP.

Passwords are not available for viewing and do not appear in clear text when entered. This requirement is the responsibility of the customer and should be handled with an SOP.

RAPID-Pharma does not use biometrics.

C-11.300

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:

C-11.300.a

Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

As RAPID-Pharma uses Windows credentials (username and password) it is the customer's responsibility to ensure that each combination of username and password is unique.

C-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).

As RAPID-Pharma uses Windows credentials (username and password) it is the customer's responsibility to ensure that the identification code and password issuances are checked periodically for all other aspects of security. RAPID-Pharma automatically inherits such checks from the Windows operating system e.g. password aging.

TABLE 1 (continued)
Regulation section

Regulation text

RAPID-Pharma Solution

C-11.300.c

Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

This requirement is the responsibility of the customer and should be handled with an SOP.

C-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.

As RAPID-Pharma uses Windows credentials (username and password) it can ensure that incorrect user names and passwords can be detected. In addition, these are logged to the audit trail.

C-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.

This requirement is the responsibility of the customer and should be handled with an SOP.

CONCLUSION

Automsoft designed and developed RAPID-Pharma in collaboration with pharmaceutical customers specifically to address the requirements of 21 CFR Part 11. This document identifies each individual requirement and the RAPID-Pharma response. RAPID-Pharma became one of the first fully Part 11 validated installations in a major pharmaceutical customer in July of 2002, becoming one of the first such validations in the world.

Automsoft specializes in developing software to manage production data, for process industries, in a highly secure environment. In this context, ensuring compliance with FDA regulations governing the management of that data is an intrinsic element of our design and development processes. Rather than interpreting requirements from regulatory authorities ourselves, we work in collaboration with our customers to develop a definition and software based implementation of the regulations. This ensures that RAPID-Pharma is designed by the industry, for the industry in a real-world context.

Automsoft recognizes Part 11 compliance as one of the most critical issues facing the FDA regulated industries. At present Part 11 applies only to the pharmaceutical, bio-tech and medical device sectors, however it may in the future apply to both the cosmetic and food industries. Automsoft are committed to supporting these sectors in achieving Part 11 compliance with the delivery of versions of RAPID taking specific account of the requirements for each sector.

North America

Automsoft
Sales, North America
330 South Service Road, Suite 120
Melville
NY 11747
USA

T +1 631 574 4922

F +1 631 574 4923

Automsoft
Professional Services
5 Independence Way, Suite 300
Princeton
NJ 08540
USA

T +1 609 919 6010

F +1 609 720 9000

Europe

Automsoft
Sales, Europe
18 Lansdowne Road
Dublin 4
Ireland

T +353-1-449 1100

F +353-1-449 1199

E info@automsoft.com

W www.automsoft.com

© Automsoft 2002

Automsoft[®]