Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Requirements of FDA's 21 CFR Part 11 and Software Programs That Meet the Requirements

With the increased use of electronic records in the Biotechnology Industry, there became a need for requirements to address data security, data integrity and traceability of this data. In response, the Food and Drug Administration (FDA) published a regulation called 21 CFR Part 11 (August, 1997.) The intent of the new regulation was also to promote the use of electronic technology. The regulation provides Biotech companies with the requirements that enable them to move toward electronic record keeping while still maint...

Copyright SANS Institute
Author Retains Full Rights

AD

The Requirements of FDA's 21 CFR Part 11 and Software Programs That Meet the Requirements

Kristine Safi
Date Submitted: November 11, 2004
GSEC Version 1.4b

© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005 Author retains full rights.

The Requirements of FDA's 21 CFR Part 11 and Software Programs That Meet the Requirements

Abstract:

With the increased use of electronic records in the Biotechnology Industry, there became a need for requirements to address data security, data integrity and traceability of this data. In response to this need, the Food and Drug Administration (FDA) published a regulation called 21 CFR Part 11, in August of 1997. The intent of the new regulation was also to promote the use of electronic technology. The regulation provides Biotech companies with the requirements that enable them to move toward electronic record keeping while still maintaining data security, integrity and audit traceability. The implementation of the requirements addressed by 21 CFR Part 11 have been slow because there have been many "questions surrounding the scope and interpretation of these regulations, the high costs anticipated by the industry, and the absence of acceptable and commercially available technical solutions." [1]

This paper provides a high level view of the requirements of 21 CFR Part 11 and then discusses a few of the commercially available technical solutions that currently exist to meet FDA's 21 CFR Part 11 requirements. Each software program is addressed individually, starting with a high level overview of the tool, including reviews from sources in the industry. Then, each tool is compared against the 21 CFR Part 11 requirements in a table for easy evaluation.

21 Code of Federal Regulations (CFR) Part 11- Introduction and Background

As stated above, the Food and Drug Administration issued the regulation called 21 CFR Part 11 to address the increased use of electronic records in the Biotechnology Industry and to promote the use of electronic technology. When the draft guidance document was published in February, 2003 many questions and concerns were raised. The Biotechnology industry felt as though the new regulation would deter companies from moving toward electronic technology and that the FDA did not consider the costs associated with compliance to this regulation when it was created. The FDA listened and removed the draft guidance document. After many revisions, in August of 2003, the FDA published the "Guidance for Industry Part 11, Electronic Records; Electronic Signatures- Scope and Application." The FDA created that guidance document to help companies "avoid unnecessary resource expenditures to comply with part 11 requirements." [2] This guidance document describes how the FDA intends to enforce this new regulation.

The scope of 21 CFR Part 11 is fairly narrow. If a company chooses to maintain records in electronic format instead of paper format, those records are subject to the rules of 21 CFR Part 11. The FDA defines electronic records as,

---

[1] Bartha, pg 60

[2] U.S. Food and Drug Administration, 21 CFR Part 11. pg 5

© SANS Institute 2005 Author retains full rights.

"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."[3] Conversely, if a company uses computers to generate paper printouts of electronic records and those paper printouts are what are used to perform regulated activities and those paper printouts comply with other required predicate rules, then the FDA does not consider those records as having to comply with the 21 CFR Part 11 requirements (US Food and Drug, 2003, pg 6).

According to the guidance document, of the records identified above, it is applicable to "records that are required to be maintained under predicate rule requirements and that are maintained in electronic format in place of paper format", "records that are maintained… in electronic format in addition to paper format, and are relied on to perform regulated activities", "records submitted to the FDA… in electronic format", and "electronic signatures that are intended to be the equivalent of handwritten signatures, initials, and other general signings required by predicate rules." [4] After reviewing the predicate rules and the 21 CFR Part 11 requirements, it would be prudent to document the reasoning for why it was determined that a certain record was deemed applicable or not applicable to the specific regulations. This could protect a company in an audit situation.

21CFR Part 11- Requirements

The fundamental requirements of 21 CFR Part 11 are the compliance with Data Security, Data Integrity, Traceability/Audit Trails and Electronic Signature rules. Each of these requirements is addressed in more detail below. The regulation also distinguishes between 'open' systems and 'closed' systems. According to the FDA a "Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system." [5]An open system, then, is "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." [6] The requirements for open systems are more rigorous than the requirements for closed systems because not only do open systems have to comply with the controls listed for closed systems but open systems must also provide procedures for activities such as ensuring confidentiality, integrity and authenticity of the electronic records. (Coffey, pg 5)

The sections of 21 CFR Part 11 are:

Section 11.10 Controls for Closed Systems
Section 11.30 Controls for Open Systems
Section 11.50 Signature Manifestations
Section 11.70 Signature/record linking

[3] Schneider, pg 1
[4] U.S. Food and Drug Administration, 21 CFR Part 11. pg 6
[5] Code of Federal Regulations, Title 21 Food and Drugs. Part 11. pg 120
[6] Code of Federal Regulations, Title 21 Food and Drugs. Part 11. pg 120

© SANS Institute 2005 Author retains full rights.

Section 11.100 General Requirements
Section 11.200 Electronic signature components and controls
Section 11.300 Controls for identification

Each section may also have several sub-sections. Particulars of the sections are discussed in the table below as well as how the tool meets the requirements.

The Software Programs

When the Federal Drug Administration (FDA) released the rule called 21 CFR Part 11, it was realized that there would be a need for some changes in the way the pharmaceutical industry handled electronic records. Several software programs have been designed to help companies come into compliance with 21 CFR Part 11. This paper will discuss the following software programs developed by various vendors for 21 CFR Part 11 compliance: RAPID-Pharma by Automsoft, NuGenesis Scientific Data Management System (SDMS), and ChemStation Plus by Agilent.

RAPID

"Automsoft is a leading global provider of advanced manufacturing intelligence systems for process industries across a range of sectors, utilizing advanced database software to collect and store, consolidate and analyze production data and bridge islands of data within the plant and the enterprise," writes Washington Business Information, Inc.[7]

RAPID is a product suite created by Automsoft. It has been around for several years and has a great reputation. RAPID is used in several different industries including Chemicals, Food and Beverages, and Pharmaceuticals/Biotech. This product provides companies the ability to deal with extremely large amounts of data that are produced while performing everyday functions. RAPID allows companies to effectively gather and consolidate the data into a manageable format in order to analyze and report on significant tasks within the company. An aspect of RAPID that consumers find very valuable is the ability to view real-time online status of their data. RAPID also has the ability to trend historical data which is made available online, on-demand.

RAPID-Pharma is a module that is part of the RAPID product suite. As with all three tools discussed here, a company would need to implement the RAPID base software in order to reap the benefits of this security module. This module has been designed to specifically address the requirements of 21 CFR Part 11 for the pharmaceutical/biotech industries. (Automsoft, pg 2) In fact, Automsoft says that, "RAPID-Pharma completely addresses the Part 11 regulation." [8] In researching information about this software program, technically it does not meet every requirement, line by line, of the regulation, but it does meet all the requirements that a tool can address. The requirements that it

[7] Washington Business Information, Inc. pg1
[8] Automsoft. RAPID-Pharma and 21 CFR Part 11. pg 1

© SANS Institute 2005 Author retains full rights.

cannot and does not meet are the requirements that relate to processes. For example, 11.10i requires that persons that are involved in electronic signatures, whether it is the development, maintenance or use, must have the proper education. This is something that should be addressed in a Standard Operating Procedure (SOP).

As stated earlier, the high level requirements of 21 CFR Part 11 are the implementation of data security, data integrity, traceability/audit trails and electronic signatures. Data Security and Integrity are addressed through the use of the Microsoft Windows security on top of which this software runs. All user ids and other security settings are managed through the pre-configured security settings in the MS Windows operating systems (NT/2000/XP) and inherited by Rapid-Pharma. There is also the ability to assign various levels of permission and privileges depending on the user's access requirements. Then, when a legitimate user or a malicious makes any changes to any of the data, a record is written to the audit trail for traceability and maintenance of data integrity.

RAPID-Pharma preserves the audit trail in a separate database. This database is linked with the software program to ensure the capture of all human interactions with the system. Automsoft has even developed the ability to audit the audit trail database. If an audit trail document is deleted, that deletion is documented in the audit trail database. Also, if by chance there were a network outage, all audit records residing on the actual RAPID-Pharma system database would be cached locally to prevent the loss of any records and then once connectivity was reestablished, all data would be sent to the audit database. (Automsoft, pg 4)

Again, leveraging the MS Windows infrastructure, electronic signatures are created using MS Windows credentials. This electronic signature is a PKI based signature generated from the Adobe Self Sign feature of Adobe Acrobat (Automsoft, pg 3). The use of an electronic signature provides evidence that the information has not been altered during transmission. 21 CFR Part 11 requires that there be three items that are part of the electronic signature that are in human readable format. Those include: signer's full name, date and time of signing and the reason for signing (Automsoft, pg 3). RAPID- Pharma complies with this requirement.

A significant benefit of RAPID-Pharma is that it is very easy to install and configure because it is a "commercial off the Shelf (COTS) software product" and "it is built on client/server technologies and runs on the Microsoft Windows family of operating systems." [9]According to Automsoft, with this product, a company can be up and running and adding value to the enterprise within 24 hours.

ChemStationPlus

ChemStation Plus is a Security Pack created by Agilent to run in conjunction with the ChemStation base software. Agilent separates the 21 CFR Part 11 requirements into three areas: Data Security, Data Integrity and Data Traceability. This software company is the only one of the three that is discussed in this paper that provides an online demo of how the tool works and how it

[9] Automsoft. RAPID-Pharma and 21 CFR Part 11. pg 5

© SANS Institute 2005 Author retains full rights.

meets the requirements. This can be very useful in determining the best tool for a company.

According to the International Conference for Harmonization (ICH), ChemStation Plus, by Agilent, "is the only pharmaceutical software available that supports automated method validation from planning to final reporting according to ICH, Pharmacopoeia and FDA guidelines, including 21 CFR Part 11." [10] This can drastically improve the productivity of a company by having all of this functionality built into one tool.

ChemStation Plus has the flexibility to use either a Microsoft Access database or an Oracle database for the storage of important data elements. When ChemStation Plus is implemented, it meets the rigorous demands of the 21 CFR Part 11 requirements of data security, data integrity, audit trails and electronic signatures.

The data security requirement is met by limiting access to the program and the backend databases. ChemStation Plus enforces the use of both a username and a password for access to the software and the data. Then, ChemStation Plus also provides the ability to assign access levels to the various users and groups. There are predefined levels of authority as well as customizable levels of authority. That is a very good option to have since it is very important to have the ability to exercise the Principle of Least Privilege. According to the SANS Security Essentials book on "Windows Security", the Principle of Least Privilege means that users should be granted "the fewest permissions and rights possible needed to permit them to get their legitimate work done." [11] Separation of Duties is employed in the setting up and maintenance of user ids. Separation of Duties is "the practice of splitting privileges among multiple individuals." [12] The database administrators are responsible for the creation and maintenance of the user ids. The database administrators give appropriate access to the users. With a Standard Operating Procedure (SOP) a company could further the rule of separation of duties by requiring management approval for creation of ids and access permissions. Users are required to change their password at first logon so passwords are only known by the user at all times.

Data Integrity means that data has been protected from unauthorized modifications. ChemStation Plus uses a 24 byte hash value digest algorithm to protect all the data stored in the database. Also, this software program uses Oracle database recovery tools to prevent accidental data loss. Data can be set to be backed up at customizable time periods, but is recommended that data be automatically backed up as frequently as possible, potentially every minute. Data versioning is an important part of Data Integrity. With ChemStation Plus, all the data is stored in one central location and automatic versioning is engaged.

The requirement of Traceability/Audit Trails addresses the who, what, when and why of data modifications. Whenever data is modified the ID of the person is captured and logged as well as what was changed, the date and time

[10] SeparationNOW.com, pg 1
[11] Cole, Book 5, pg 82
[12] Cole, Book 2, pg 143

© SANS Institute 2005 Author retains full rights.

and the reason for the modification. All of the audit trail data is printed in human readable format and no data can be omitted.

Lastly, the electronic signature requirement in the regulation states that it must be composed of two identification components that are used to authenticate who the signer is. ChemStation Plus uses the user ID and password for manifestation of the signature. This is then linked back to the document. It is not stated in the ChemStation Plus White paper or other available documentation whether or not Agilent makes use of PKI technology to maintain authenticity.

Like most products, ChemStation Plus is designed and supported for only a closed system; however, Agilent does provide very good documentation and guidance, as well as Agilent-certified engineers that can provide additional services for ensuring compliance with the open system regulations. Many reviews boast about how well the ChemStation Plus module with the added 21 CFR Part 11 upgrades integrates with the whole stand alone ChemStation software program. The White Paper that Agilent has created for this product is very insightful. It goes into minute detail of how the software meets each of the requirements of 21 CFR Part 11. This can be found at http://www.chem.agilent.com/cpdocs/A10681.pdf .

NuGenesis Scientific Data Management System (SDMS)

NuGenesis SDMS is a software program that is slightly different from the other programs discussed here in that it does not contain a separate module that addresses the requirements of 21 CFR Part 11. Instead, it meets most requirements in and of itself while performing several other functions, meeting predicate rules and creating new efficiencies for a company. A few of the Part 11 requirements do require an additional module or two from the NuGenesis product line for complete compliance (see table below for specific requirement information). This product integrates seamlessly with existing scientific and IT infrastructures. It is able to integrate with all existing analytical equipment.

Chemistry Today published an article called "Cycle time reduction in manufacturing using a scientific data management system." In this article they commend the Nugenesis SDMS software program as being an effective "process-streamlining tool" that many large biotech firms have deployed to reduce cycle time in manufacturing and come into compliance with 21 CFR Part 11. The article goes on further to say that "Implementing NuGenesis SDMS at manufacturing locations where a company is racing against competitors can also provide a strategic competitive advantage." [13] The three key benefits to using NuGenesis SDMS are its usability, its scalability and it "enhances the 'metadata' core environment for data searching and retrieval." [14] Another benefit of NuGenesis SDMS, is that it has made a lot of strategic headway in the industry by collaborating and integrating with other influential software and instruments in the industry, indicates Scientific Computing.

[13] Lander, Victoria. pg 14
[14] Lander, Victoria. pg 14

© SANS Institute 2005 Author retains full rights.

The main requirements, as stated previously, of 21 CFR Part 11 are data security, data integrity, traceability/audit trails and electronic signatures. Data security and data integrity are maintained by requiring users to login with a valid user name and password. There are then permission tables that delineate what a user has access to and what that user has the ability to do. Anything that is done with the data is logged to the audit trail, thus maintaining the integrity of the data.

Capturing the who, what, when and why of data modifications is the requirement of the traceability/audit trails requirement. This data is captured automatically and includes the user id, the date and time, and what was modified. The data that is not captured is why the data was modified. This data cannot be modified. It is all permanent and readily available in human readable format.

NuGenesis SMDS meets the minimal requirements that are defined in 21 CFR Part 11. The requirements are very simple and state that two identification components are required; username and password are used here. Then, the electronic signature must be in human readable format and include the name of the signer, the date and time of the signature and the reason for signing. This software tool does ensure that electronic signatures are unique to the individual and that there is no reuse of signatures.

In comparing the tools, NuGenesis SDMS appears to be the only one with built in notification system of unauthorized attempts to access the system. This is stressed as an important requirement of the regulation (11.300.d**)**. NuGenesis sends out notifications to a Monitor as well as logs the events in the audit trail. The other two tools examined here only log the events in the audit trail. There is no built in notification.

Conclusion

The implementation of the 21 CFR Part 11 regulation may be costly and require a lot of work, but it has standardized and created control for the handling of electronic records. This regulation is leading to more efficiencies and productivity within companies. Ultimately, this regulation will also reduce product time to market which is better for producers, manufacturers and consumers.

As stated earlier, the four fundamental requirements of 21 CFR Part 11 are Data Security, Data Integrity, Traceability and Electronic Signatures. Each company thoroughly addresses the requirement of data security by limiting access to the software program and the backend databases that stores the information. They even allow for the creation of different access control levels so users can only access data that is at their assigned level of permissions fulfilling the Principle of Least Privilege. Even though the software programs themselves are considered closed systems, all companies did assume that their software program would also be implemented within a closed system, meaning that a malicious user would not even be able to capture data across the network.

Data Integrity is also addressed by all three companies. In conjunction with the Data Security requirement, data integrity can be maintained because access to all data is restricted to authorized persons only and modifications to the data are even more limited. There is strict change control enforced in each

© SANS Institute 2005 Author retains full rights.

software program. All changes to all data types (raw and meta) are documented. This is very important, especially in an audit situation, which leads to the next requirement, Traceability.

In all three tools, any modifications to all data types are tracked including who, what, when and why. All tools capture the user ID that made the changes, what was changed, when (date and time) the modification was made and why- the user is required to enter a reason for the modification. All of this information is readily available in human readable format and never hidden or omitted.

Electronic Signatures are dealt with slightly differently in the tools and this comes from the fact that the requirement is specific, but slightly lacking. The requirement states that all that is needed are two identification components to sign a document and that the signer's name, date and time of signature and the reason for signing are presented in human readable format. Automsoft took it a step further and also implemented PKI technology which allows for the ability to prove authenticity of a document. All software programs that are in this industry should utilize this technology for better integrity and security of documents.

All three of the software programs discussed here are used in the industry. Companies that have chosen each of these software programs have successfully passed FDA inspections. There are pros and cons to each of these software programs, which is to be expected. It comes down to what is important to a particular company and what their business requirements and objectives are.

© SANS Institute 2005, Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced