OMRON

Automated Manufacturing in the Food & Drugs Industry

An Introduction to the Regulations

SCOPE

The Food & Drugs industry has many standards and guidelines that need to be followed; these can bring on a lot of new questions about the hardware and software used. This white paper gives a basic introduction to the standards and how Omron products can be tailored to suit these requirements with a focus on the software and automated manufacturing. It is expected that the reader will already have a basic technical knowledge of Omron software and hardware. Previous knowledge of Food & Drugs regulations is not expected.

CONTENT

Executive Summary **2**
1 Introduction **3**
2 What is 21 CFR Part 11 ..... **4**
3 What about the EU GMP Guidelines? **5**
4 Who needs to follow EU or US regulations and Guidelines? **5**
5 Omron Products for 21 CFR **6**
6 The Way Forwards **12**
7 Appendix 1 21 CFR Part 11 ..... **12**
8 Appendix 2 Eudralex GMP Annex 11 ..... **17**
Computerised systems **17**

WHITEPAPER

Executive Summary

In order to reduce accidents and injuries caused by contaminated or badly produced food or drugs most nations around the world now have strict regulations for manufacturers to follow and stiff penalties for those who fail to ensure that relevant products are safe and uncontaminated at the point of consumption.

The US has a regulation known as 21 CFR, this is perhaps the most widely known set of regulations for the pharmaceutical industry and is often used as a benchmark worldwide especially where the supply chain involves or ends up in the USA. In Europe, there are some guidelines known as GMP and GAMP which are used when manufacturing products for the pharmaceutical industry, these are implemented in the regulations and statutes for individual member states within the EU.

Failure to comply with the local regulations can result in production being stopped, expensive litigation and the cost of recalling potentially dangerous products from the market. Likewise, keeping careful records can minimise the impact on the business should there be a problem.

Individual products and suppliers cannot be 'compliant' with these standards or regulations. The end solution must be compliant and validated based on how it is developed and what design decisions take place during the development. This white paper summarises the better known standards and regulations investigating the implications of this when using Omron hardware and software in the pharmaceutical and medical industries.

1 Introduction

By far the most well know of the Food and Drugs standards is the USA one, known as 21 CFR. The Code of Federal Regulations (CFR) Title 21 is a large group of regulations specifically aimed at products for human consumption. These regulations are maintained and policed by the Food and Drug Agency (FDA) in the USA and around the world where products are destined for US markets. The regulations cover a diverse range of things from food, drink and medicine to artificial limbs and regulations on trial of drugs, tissue transplanting and even marketing of the products.

Providers of automation solutions for the food and drugs market are increasingly being put under pressure to understand and by able to conform to regulations set out in 21 CFR. This is particularly important if working with applicable products in the USA but these regulations and other similar standards from other authorities are being used throughout the world and often not just in the food and drug industry.

One part of the FDA specification known as 21 CFR part 11 relates to the storage and security of electronic records created during the manufacturing process and specifically how these records can be trustworthy and reliable. Other parts of 21 CFR stipulate exactly what needs to be recorded for a particular product; part 11 stipulates how to ensure this can be trusted.

In the European Union there is a list of rules known as EudraLex. These rules are then taken into the law of member states together with any other local regulations that may apply. The EU rules have a large overlap with the USA CFR regulations although conforming to one country's regulations does not mean you necessarily conform to another's. The rules concerning computerised systems for Pharmaceutical and Veterinary use can be found in EudraLex GMP (Good Manufacturing Practice) Volume 4 Annex 11 (See Appendix 2 Eudralex GMP Annex 11).

For the purpose of this document we will focus on the FDA 21 CFR part 11 regulations as they have been the cause of a lot of confusion since their introduction. Also, as a supplier to the pharma industry, part 11 is an area where Omron can really help customers.

This document aims to explain what 21 CFR part 11 is, how it affects end users, OEMs and solution providers and how Omron can provide specific products which help system designers to create systems that comply with relevant 21 CFR regulations.

The entire 21 CFR part 11 can be found in Appendix 1 21 CFR Part 11. The regulation itself is not lengthy, but this can lead to much confusion about details of how the regulations can be implemented. This is further complicated by the European pharma guidelines which will apply to any Omron customers working within Europe – the computer systems guidelines can be found in Appendix 2 Eudralex GMP Annex 11.

As a supplier it is our duty to our customers and potential customers to gain an understanding of their regulatory burden and help where possible by being knowledgeable, understanding and supplying products that will aid conformity to the regulations.

2 What is 21 CFR Part 11

21 CFR Part 11 is a list of regulations (Code of Federal Regulations) regarding the use of electronic storage of records relating to the manufacture of food and drugs. This title is written in many ways including CFR 21 11 and CFR 21 part 11. For the purpose of this document we will call it "21 CFR Part 11".

The main aim of these regulations is to ensure that any data saved as a result of the manufacturing process is trustworthy and reliable. For many years manufacturers were forced to keep verbose signed paper records in order to allow traceability of a manufacturing process. The automation of these processes and increased electronic storage possibilities forced the advent of a new standard.

21 CFR Part 11 doesn't regulate what needs to be stored electronically; it just regulates how secure and trustworthy electronic logs (if any) are. The information that needs to be saved or stored is defined in the part of 21 CFR that applies to the particular product being produced – for example 21 CFR Part 211 contains the regulations for manufacturing 'Finished Drugs' which includes the need to keep an audit trail of key data– keeping this electronically brings the application into the scope of Part 11.

It is the duty of the manufacturer to ensure that the relevant regulations have been followed. The whole of 21 CFR is checked and enforced by spot checks from the FDA and if something is deemed to be non-compliant, the manufacturer is given opportunity to resolve the issue, respond or in certain serious cases production is stopped an product recalls can be forced.

Most parts of 21 CFR require what is known as an audit trail, this is documented evidence of all significant changes to a machine, its configuration or key information regarding individual products manufactured. This audit trail is needed so in the event of a problem, the records can be checked by the company or enforcement agencies to ensure that any recalls apply to the correct batches and that someone can be held responsible for the problems and if needed be re-trained.

As the information stored in audit trails can contain important information which could decided which products are recalled or other important safety information, it is essential that they cannot be modified or tampered with in any way. Integrity of the data is essential.

Electronic storage of records is prone to modification by mistake or deliberately - especially as the information has the capacity to be incriminating. So an aim of 21 CFR Part 11 is to attempt to make electronic records and signatures as trustworthy as the old fashioned paper which was almost impossible to modify after it had been created without being detectable.

It is possible to bypass some 21 CFR part 11 regulations by ensuring that all records and logs are created as paper copies. Although this is increasingly hard to guarantee as the 'original' copy if the computer system is also storing electronic logs.

21 CFR part 11 requires that all data important to the traceability of a system is saved to a file which cannot be modified after the log has been created, commonly this can be a database or in some systems a bespoke, encrypted file. These requirements are the bulk of 21 CFR part 11 and can be seen in Appendix 1 21 CFR Part

11Subpart B—Electronic Records (In particular 11.10 e).

The regulations also require that the security of the system can be ensured – and therefore that the logs cannot be modified or deleted. This means the user must only be permitted to do what they are required to do, thus each user has access to a specific level of functionality and are unable to gain access to any other part of the system or the computer running the process. Users logging into the computer system must have secure passwords that last for a set period of time before needing to be reset (See Appendix 1 21 CFR Part 11 -11.10 Controls for closed systems (g and i) and Subpart C—Electronic Signatures - 11.300 Controls for identification codes/passwords.

PCs or similar machines where the background operating system (e.g. Windows) could allow users to tamper with the machine without any record of this breach are particularly important to protect. For example in Windows it may be necessary to disable all operating system short cuts and toolbars so the normal user can only control the foreground software required for the manufacturing process. See Appendix 1 21 CFR Part 11 -11.10 Controls for closed systems (d, g and i).

3 What about the EU GMP Guidelines?

In the EU there are some guidelines for computers used in manufacturing which are similar to the 21 CFR part 11 standard, although the FDA regulations are much more explicit than the EU ones (See Appendix 2 for the EU GMP Volume 4 Annex 11 on Computer Systems). Part 10 of the EU Guidelines covers the need for an 'audit trail' of any changes made to the system, part 13 aims to ensure that the stored data cannot be tampered with either by accident or wilfully. Part 8 of the Annex ensures that only authorised users can work with a system. These all have parallels in the 21 CFR Part 11 Regulations.

It should be noted that the EU documents are 'guidelines' and the 21 CFR documents are 'regulations', the EU documents are made law by the member states. This is highlighted by the use of words like 'should' throughout the EU guidelines.

4 Who needs to follow EU or US regulations and Guidelines?

By law, anyone manufacturing Food or Drugs in the USA must have followed the appropriate parts of 21 CFR including part 11 if appropriate. 21 CFR is also required by food and drug manufacturers outside the USA who have operations in the USA or market in the USA and increasingly food and drug companies worldwide are following the regulations even when not required to by US laws.

In the EU the customer must follow the regulations for the particular member state(s) where they market and operate. These may have more stringent regulations than in the EU GMP Guidelines so care must be taken to understand exactly what is required.

An understanding and conformance to these guidelines and regulations will become increasingly needed as we work more with pharmaceutical customers.
As a provider to OEMs Omron needs to offer products that allow the OEM to create systems that can be conform to the relevant regulations and also be able to highlight how this can be done. Omron must also be able to provide details of our quality systems should the customer require an audit of this.

Any company working with and maintaining a machine which produces a product that falls under these regulations is responsible for following the regulations, these companies are generally Omron 'end users'. If Omron is ever supplying these customers, we should maintain an understanding of the regulatory pressures the customer has. As with other industrial sectors, Omron's core competence remains with working with OEMs who supply the end users this also removes some of the burden of compliance from Omron.

Outside the food and drug industry traceability and reliable records are also becoming increasingly important especially where safety, profitability or 3rd party assets are at risk. The historical records can also be used to improve manufacturing processes and highlighting problems either physically with the process or highlighting areas where employees can be trained or improved.

5 Omron Products for 21 CFR

Each application created has to conform to all relevant 21 CFR regulations, including part 11 where applicable. It is not possible for individual software or hardware components to be 'certified' as compliant, in fact there are no standards for hardware or software that must be fulfilled unless specified by a particular customer or the machines will be working in a 'clean' zone.

Omron usually provides products rather than complete applications to customers so the aim is to provide functionality within the relevant products that allows our customers or OEMs to comply with 21 CFR regulations for their final applications.

Generally, for the hardware side, our assistance is limited to working with the customer to help them create their application – 21 CFR Part 11 is rarely applicable within a PLC or its programs. We should always be aware of the regulatory load on our customers. For example, a simple firmware upgrade or a small PLC program change could cause many hours of paperwork and risk assessments purely to manage the change. Without this, problems resulting from the 'minor' change could result in criminal negligence proceedings for our customer – and potentially litigation for Omron!

5.1 CX-Supervisor v3.1

From version 3.1 CX-Supervisor has functionality which helps end applications conform to 21 CFR part 11 and is available as a free upgrade to v3.0 users.

This functionality comes in three parts which can be used separately to each other as required by applications although careful planning and thought must go into making an application conform to 21 CFR Part 11. Simply using a capable software package does not make your resulting application compliant.

5.1.1 Audit Trail To Database

CX-Supervisor now has the ability to create a detailed audit trail to a secure database, either using MS Access or an SQL database. The choice of database depends on how comfortable application developers feel with different databases and also how related systems are working. Many 21 CFR part 11 compliant systems use SQL for storing the audit trail but Microsoft Access is much easier to setup and configure to quickly have a working system, MS Access files are automatically password protected by CX-Supervisor which provides protection against all but the most malicious breaches of security.

Each point in CX-Supervisor can be configured to create an audit trail, so when the value of the point changes, the information is logged, including before and after values, the currently logged in user, the date and time of the change and an ID which can show a batch number or similar. Careful selection of which points to audit in a project can give a good picture of what is happening in a system. The developer should be careful to ensure that any points that are intended for the audit trail are not updating so frequently as to slow the system down with the amount of data logging and producing so much detail that it becomes too cumbersome to use. Obviously, these decisions must be made in accordance with what is required for a project under the relevant 21 CFR part.

Alarms can be configured to be logged to the same audit trail database in addition to them going to the standard textual alarm log. The alarms which are logged to the audit trail can be selected individually or the developer can choose to log all alarms to the audit trail. This is important for building up a picture of what has happened to a system.

FDA auditors would require an end user to demonstrate that they have addressed all known risks that would result in a compromised audit trail. These risks include malicious users and accidental modification of the records. A PC system has inherent security issues and someone could modify data given time and inclination. The job of the end user is to understand these risks and reduce them to an acceptable level for their system. The Microsoft Access solution is great because no-one knows the password to modify the data, however there may be risks that those with sophisticated tools could potentially modify the database and with sufficient access writes could delete the database altogether. In order to reduce this risk it is important that only trusted users are able to access the file and that suitable back up procedures are put in place and documented.

5.1.2 Login Using Windows Credentials

The Microsoft Windows password handling allows users to add rules for password aging and password complexity. These rules can be applied throughout an organisation's computer systems including uniqueness of user Ids which is not possible on a standalone password manager. All of these are essential when following 21 CFR part 11 regulations (See Appendix 1 21 CFR Part 11 - 11.300 Controls for identification codes/ passwords).

CX-Supervisor now allows you to configure a user to have their password checked against the Microsoft Windows passwords. This ensures that not even the application developer is able to see the login password and that the organisation's policies regarding passwords are echoed within CX-Supervisor.
CX-Supervisor has always offered different user levels where a user type can do things that another user cannot do. These user levels can be used within the application to enable and disable features e.g. pages of the project or buttons.

5.1.3 Ensuring the user only does what they are supposed to do

See Appendix 1 21 CFR Part 11-11.10 Controls for closed systems (d, g and i). If using a touch panel without a keyboard and mouse, its much easier to ensure that the user cannot gain access to the computer in the background. CX-Supervisor can be made a full screen application and only by exiting (which can be disabled) can a user get access to the operating system and potentially damage the audit trail logs.

If using a keyboard, there are more things to consider as they keyboard is usually able to bring up things such as the Windows 'Start' menu or the Ctrl-Alt-Del menu.

The disabling of the various Windows shortcuts/hotkeys is achieved using various registry changes and changes to the policies of the local machine. Depending on requirements it is even possible to get Windows to start CX-Supervisor instead of Windows Explorer.

5.1.4 Special Considerations When Using CX-Supervisor to Generate an Audit Trail

The amount of data generated by an audit trail depends on how much is being audited and how fast the machine creates products. For example a machine which fills 10 bottles a second will potentially generate audits at the rate of several audit points every 100ms.

Data communications at this speed effectively rule out all network types other than Ethernet based, even with Ethernet, care must be taken to not overload the system based on data throughput and cycle time of the PLC – more information on this is available in the user manual of CX-Supervisor.

The designer of the system must ensure that the generation of the audit trail does not compromise system stability or network throughput, it is wise to follow these guidelines:

- Only Audit what you need when you need – keep frequently audited items to an absolute minimum.
- Keep points for each 'audit' in an area of contiguous memory
  - For example, if multiple audits are generated when an item has been made, make sure they are in d1-10 – or better stored as an array.
- Keep the update rate for the points being audited as slow as possible to ensure all data is captured while not overloading the system
- Consider storing multiple audits in the PLC and sending a trigger to CX-Supervisor to download and process them in a single message.
- Consider using the SPU if high speed and high accuracy are required beyond the capability of an Ethernet network. (See Section 5.3 SPU for more information)

5.2 Xpectia

The Omron vision system Xpectia has also implemented functionality required to ensure an end system can be compliant with 21 CFR Part 11.

The following items are written to a log for retrieval at a later stage:

- Configuration data - Configuration data with change history can show the inspection method at a certain point in time
- Logging image - The image taken by the vision system is saved with time stamp showing the appearance of each individual product.
- Logging data - Logging data with time stamp shows the inspection result of each individual product

The configuration of Xpectia is only allowed by an authorised user and access to the configuration files is restricted from accidental or deliberate tampering. Any changes to the configuration are logged with a timestamp and the previous revision is kept. The revision number of the configuration is shown.

Xpectia also supports batch reporting of the following:

- Batch / Lot No
- Start date and time
- User ID of starter

- End date and time
- User ID of ender
- PASS/FAIL counts for each camera
- configuration data

During a batch Xpectia accepts a trigger signal to perform an inspection. At the end of a batch the user can export the batch report, the logging data and images are also attached to the report for completeness.

The integrity of the saved records is achieved by ensuring that export and import can only be achieved using an encrypted file which can be viewed and printed using a Data Viewer application on a PC. Nothing can modify the records.

5.3 SPU

Sometimes, the quantity of data required to be logged and the accuracy required with timing exceeds that which CX-Supervisor and the network which attaches it to the PLC can manage reliably.

In this situation Omron has a CJ PLC module known as the SPU – Storage and Processing Unit. The SPU is a high speed device which is physically attached to the PLC. The SPU can log data at an extremely high rate to a memory card inside. Separate software known as EDMS is available which can read from the SPU storage and transfer to a secure SQL database – It is possible to use the same SQL database used by CX-Supervisor if a mixture of detailed Visualisation logging and high speed PLC level logging is required.

5.3.1 How the SPU Works

The SPU simply allows PLC memory areas or points to be logged at regular (as frequently as 7ms) intervals or when triggered to do so. These memory areas could be values that the PLC has measured, or could be items that a user has set within a visualisation package such as CX-Supervisor or on an HMI such as an NS Terminal.

The SPU physically attaches to the PLC so has no network issues when getting information directly from the PLC memory – the data is available in an instant.

The SPU comes complete with an Ethernet port which enables an external PLC to take the information from the SPU memory and process. EDMS software enables this to be done automatically.

5.3.2 SPU Security

The SPU contains some features which allow you to browse the internal storage card and view and potentially edit the log files it creates from a normal Windows PC. This feature can be a problem for users intending to use it for a 21 CFR part 11 application as this represents a security risk. The SPU can be configured to disable this feature so it is not possible to browse or write to the SPU using this method. However, enabling and disabling this feature does not require a password. In order to mitigate against this risk it is advisable that in situations that require high levels of data integrity and security (i.e. anything for pharma industry especially where 21 CFR Part 11 is followed) the following precautions are taken:

- Ensure that the SPU and PLC are in a locked cabinet
    - The Compact Flash card in the SPU contains editable data so must be protected
- Use EDMS to transfer the data from the SPU to a secure SQL database at as high a speed as is possible given the data
    - Once the data is in SQL it is managed and is protected against malicious or accidental modification – the length of time between the collection of the data and when it is stored in SQL is a potential risk to integrity.

- Disable the ability to browse to the internal storage of the SPU
  - This can be done by disabling the browse feature
- For extra security the SPU and the EDMS software should be on a closed network so no browsing or modification is possible.
- The SPU Console Utility is not password protected so the SPU can be modified if access can be gained via the network
- EDMS PC could have 2 network cards – one for SPU and one for normal network, this would enable the PC to gather the data from the closed network and log it to a secure SQL server elsewhere.
  - If the SPU and the PC running EDMS are in the same secure place this virtually eliminates accidental or deliberate tampering.

5.4 NJ with Database Connection Service

The NJ range of machine controllers don't use an add on module to perform high speed database access, there are NJ models capable of supporting high speed database communications directly to an Oracle or MS SQL Server database from within the controller. These NJ models are known as 1320, 1420 and 1520.
The NJ with database connection service uses function blocks available within Sysmac Studio to communicate with the database and Sysmac studio provides the ability to configure the database settings, there is no need to purchase additional software.

5.4.1 How NJ with Database Connection Service Works

With the correct controller version with Database connection features, Sysmac Studio has an extra configuration section to configure a database connection. Once entered and transferred to the controller the connection can be tested.

Sysmac Studio provides the developer with a set of function blocks to use in project. These include the ability to connect to, write to, read from the configured database. The calls to these functions be anywhere within the program. It is likely that, for a project related to 21 CFR Part 11 that the majority of the database use will be writing operations (i.e. for an audit trail).

If the database is not available or the network cannot keep up with the writes, the NJ writes the SQL commands to a spool within the non-volatile memory which will write to the database when the database is available. The number of SQL commands that can be spooled will vary by the length of the SQL command, there is 1MB of memory set aside for this purpose. This memory is internal to the NJ so cannot be compromised by removing the SD card.

5.4.2 NJ with Database Connection Service Security

Once your project has been synchronised with the NJ it is important to make sure no unauthorised users can upload the project and (importantly) database settings and password details from the controller. This could allow a user to create their own NJ Program to wipe incriminating data from the database. This can be achieved by Setting up Operation Authority on the NJ controller and ensuring that only people with permission have authority greater than 'Operator' or 'Observer'. (See Section 8.3 of Sysmac Studio Operation Manual).
With the Operation Authority configured, the controller is not a weak link and a user obtaining access to the device is not a problem as no data could be modified as a result. However, the reliable operation of the NJ

controller is part of the integrity of the system, so keeping it behind locked doors is advisable!

The database configuration is only as secure as the users and passwords that have access to the data. Microsoft SQL Server allows the admin user to configure that usernames and passwords obey criteria including password aging and complexity. It should be noted that if a password ages and needs changing the NJ Controller Program will also need updating in order to continue using the database. Users of the database data must only be given read access to the data so nothing can be tampered with.

5.5 Mixing Products and Audit trails

Sometimes, when creating a full solution, that there may be multiple parts to it and maybe different places can come under regulations in 21 CFR Part 11 or other standards.
It is important to plan these cross-over areas when you design the system and consider the effects on things such as audit trails.

Some things to consider:

- Clock time
  - If using multiple components in a system such as CX-Supervisor, NS, PLCs, Machine Controllers, Xpectia or an SPU in a system and potentially logging data from all these sources, it is important that the clocks are synched between the different devices so the audit logs can be matched up with each other. Some devices, such as the SPU, automatically sync with the PLC clock. It is important to understand how and when this is done (See Appendix G of SPU Console Operation Manual for further information on SPU syncing)
- Storage medium
  - CX-Supervisor has the option to write to an Access or an SQL database. When writing to an Access database, the write permissions are locked and unknown to anything other than CX-Supervisor. If multiple sources of data need to be audited to the same database, it is important to choose one which is secure but can be written to by all components that need to audit.
- Security
  - A system is only as secure as its weakest part. If CX-Supervisor is completely secure but use of another component opens up a loophole that allows a PC or another component to be compromised, the whole system is vulnerable.
  - Network cables between devices are always a risk. The most secure system is in a secured box. The effects of adding an extra device (e.g. laptop complete with Omron configuration software) to the system need to be risk assessed and acted on if appropriate.

6 The Way Forwards

Omron is not be able to create 'compliant' hardware or software for any of the regulations but we are able to help customers to make their own solutions conform to the regulations under which they are bound. Omron can first help by understanding the weight of the regulations and understanding where they apply or don't apply, by showing this knowledge we can become useful to customers and this knowledge can become a differentiating factor in what we offer.

Omron can also understand the customers better with regards to the impact of how we work affects how the customer works – for example with change control or being ready to answer questions about our quality control processes when potential customers ask.

Omron's pharmaceutical and medical customers, and target customers have a huge weight of regulation on them. This is something that we, as a supplier, can help with.

7 Appendix 1 21 CFR Part 11

This appendix contains the entire 21 CFR Part 11 Regulations. Other parts of the 21 CFR Regulations and further information can be obtained from the FDA Website:
http://www.fda.gov/
Authority: 21 U.S.C. 321–393; 42 U.S.C. 262.
Source: 62 FR 13464, Mar. 20, 1997, unless otherwise noted.
Subpart A—General Provisions

- 11.1 Scope.
- 11.2 Implementation.
- 11.3 Definitions.

Subpart B—Electronic Records

- 11.10 Controls for closed systems.
- 11.30 Controls for open systems.
- 11.50 Signature manifestations.
- 11.70 Signature/record linking.

Subpart C—Electronic Signatures

- 11.100 General requirements.
- 11.200 Electronic signature components and controls.
- 11.300 Controls for identification codes/passwords.

Subpart A—General Provisions

11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations.

However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

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

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

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004]

11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

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

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S–0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

11.3 Definitions.

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

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

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

(2) Agency means the Food and Drug Administration.

(3) Biometrics means a method of verifying an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

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

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

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

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B—Electronic Records

11.10 Controls for closed systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

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

(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.

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

(d) Limiting system access to authorized individuals.

(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.

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

(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.

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

(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.

(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.

(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.

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.

11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) 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).

11.70 Signature/record linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Subpart C—Electronic Signatures

11.100 General requirements

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

(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.

(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.

(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.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

11.200 Electronic signature components and controls

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

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

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

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

11.300 Controls for identification codes/passwords

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.

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

(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.

(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.

(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.

8 Appendix 2 Eudralex GMP Annex 11

This appendix contains the EU EudraLex GMP Volume 4 Annex 11 guidlines for Computer Systems. Other parts of the Eudralex guidlines and further information can be obtained from the EU Public Health Website: http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm

Volume 4 of "The rules governing medicinal products in the European Union" contains guidance for the interpretation of the principles and guidelines of good manufacturing practices for medicinal products for human and veterinary use laid down in Commission Directives 91/356/EEC, as amended by Directive 2003/94/EC, and 91/412/EEC respectively.

COMPUTERISED SYSTEMS

Principle

The introduction of computerised systems into systems of manufacturing, including storage, distribution and quality control does not alter the need to observe the relevant principles given elsewhere in the Guide. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality or quality assurance. Consideration should be given to the risk of losing aspects of the previous system which could result from reducing the involvement of operators.

Personnel

1. It is essential that there is the closest co-operation between key personnel and those involved with computer systems. Persons in responsible positions should have the appropriate training for the management and use of systems within their field of responsibility which utilises computers. This should include ensuring that appropriate expertise is available and used to provide advice on aspects of design, validation, installation and operation of computerised system.

Validation

2. The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether the validation is to be prospective or retrospective and whether or not novel elements are incorporated. Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and modifying.

System

3. Attention should be paid to the siting of equipment in suitable conditions where extraneous factors cannot interfere with the system.
4. A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures.
5. The software is a critical component of a computerised system. The user of such software should take all reasonable steps to ensure that it has been produced in accordance with a system of Quality Assurance.

6. The system should include, where appropriate, built-in checks of the correct entry and processing of data.
7. Before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results. If a manual system is being replaced, the two should be run in parallel for a time, as a part of this testing and validation.
8. Data should only be entered or amended by persons authorised to do so. Suitable methods of deterring unauthorised entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals. There should be a defined procedure for the issue, cancellation, and alteration of authorisation to enter and amend data, including the changing of personal passwords. Consideration should be given to systems allowing for recording of attempts to access by unauthorised persons.
9. When critical data are being entered manually (for example the weight and batch number of an ingredient during dispensing), there should be an additional check on the accuracy of the record which is made. This check may be done by a second operator or by validated electronic means.
10. The system should record the identity of operators entering or confirming critical data. Authority to amend entered data should be restricted to nominated persons. Any alteration to an entry of critical data should be authorised and recorded with the reason for the change. Consideration should be given to building into the system the creation of a complete record of all entries and amendments (an "audit trail").
11. Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approving and implementing the change. Such an alteration should only be implemented with the agreement of the person responsible for the part of the system concerned, and the alteration should be recorded. Every significant modification should be validated.
12. For quality auditing purposes, it should be possible to obtain clear printed copies of electronically stored data.
13. Data should be secured by physical or electronic means against wilful or accidental damage, in accordance with item 4.9 of the Guide. Stored data should be checked for accessibility, durability and accuracy. If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate to the storage medium being used.
14. Data should be protected by backing-up at regular intervals. Back-up data should be stored as long as necessary at a separate and secure location.
15. There should be available adequate alternative arrangements for systems which need to be operated in the event of a breakdown. The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them. For example, information required to effect a recall must be available at short notice.
16. The procedures to be followed if the system fails or breaks down should be defined and validated. Any failures and remedial action taken should be recorded.
17. A procedure should be established to record and analyse errors and to enable corrective action to be taken.
18. When outside agencies are used to provide a computer service, there should be a formal agreement including a clear statement of the responsibilities of that outside agency (see Chapter 7).
19. When the release of batches for sale or supply is carried out using a computerised system, the system should allow for only a Qualified Person to release the batches and it should clearly identify and record the person releasing the batches.

Omron Corporation

- 50 years in industrial automation
- Over 35.000 employees
- Support in every European country
- Over 1.800 employees in 19 European countries
- 800 Specialised field engineers
- 7% of turnover invested in R&D
- More than 200.000 products
- More than 6.950 patents registered to date

Omron Industrial Automation

Headquartered in Kyoto, Japan, OMRON Corporation is a global leader in the field of automation. Established in 1933 and headed by President Hisao Sakuta, Omron has more than 35,000 employees in over 35 countries working to provide products and services to customers in a variety of fields including industrial automation, electronic components industries, and healthcare. The company is divided into five regions and head offices are in Japan (Kyoto), Asia Pacific (Singapore), China (Hong Kong), Europe (Amsterdam) and US (Chicago). The European organisation has its own development and manufacturing facilities, and provides local customer support in all European countries. For more information, visit Omron's Web site at www.omron.com.

AUTHOR

Andy Avery
Product Engineer Software

- Omron Europe B.V.
  Product Marketing
  Automation department
- Fareham
  United Kingdom
- Tel. +44 (0)1489 563 804
- andy.avery@eu.omron.com
- industrial.omron.eu

Andy Avery joined Omron in 2005 as an experienced software engineer working mainly on visualisation software such as CX-Supervisor. In 2007 Andy became a product specialist, focussing on visualisation software, HMI hardware and IPCs.

The role of software in automation is huge, and increasing. This has given Andy the opportunity to use his past experience and research some of the areas that need more attention such as the pharmaceutical industry. Andy worked closely with large pharmaceutical customers to help develop solutions that could be compliant with the relevant regulations. He also worked with the Omron development teams to ensure Omron visualisation software could support the extra requirements of this industry. This white paper is a summary of the research and the implications on existing and future hardware and software in this demanding industry.