Nalys
Sense & Passion

What is *the* biggest concern when working with old equipment?

Last update: 2016.10.06

1 Contents

2 Introduction ... 1
3 Data ... 1
4 Discussion ... 3
5 Conclusion ... 4
6 References ... 4
6.1 Additional reading and information ... 5
7 Authors ... 5

2 Introduction

When working with old and ageing equipment and computer systems, many immediate concerns comes to mind; availability of spare parts, operational reliability, lack of hard- and/or software support from the supplier to name a few of the obvious. However, few remembers the major issue currently faced by many old pharmaceutical production sites face, namely the issue of data, data integrity, and electronic records.

The rapid development of computer systems and their capacity to generate, log, and store information about the process and the outcome of any given batch production, have given computer systems an increasingly important role in modern pharmaceutical productions. However, when does the information logged by the computer system become data? when does the data become GxP-data? how can we trust the integrity or rather validity, of the data? and finally how can we document that the requirements to the data, imposed by the authorities are met.

This paper will try to combine the information available from FDA (US Food and Drug Administration) and EMA (European medicines Agency) along with experience gained from working in an old production site, with the aim of raising awareness about the issue.

3 Data

The following will try to elaborate on the definitions of data stated by FDA and EMA, and put them in relation to the data flow in typical computer systems in a production.

One of the important discussion points is what is *data*?

From the Miriam-Webster dictionary, there are three definitions of data, ref. [I];

1: factual information (as measurements or statistics) used as a basis for reasoning, discussion, or calculation…

2: information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful

3: information in numerical form that can be digitally transmitted or processed

Definition 1, in GxP, can be translated to the data, which is used make a release – do-not-release decision, i.e. the final batch report.

Definitions 2 and 3 becomes more tricky when translated, as these definitions means that *all* information transmitted from any given sensor coupled to a GxP critical system becomes raw data, and as such are under the same regulation and retention restrictions as "old-school" hand-written batch documentation.

According to the collected definitions above, all information gathered by a GxP critical system during production may in fact, depending on the inspector or auditor, be considered as GxP data in one form or another.

The key issue in the discussion is the integrity or validity of the data, submitted to authorities for product approval, or used by the production to document that any given product falls within the specifications.

However, the question about data integrity does not only apply to the data stated in batch documentation, nor is the requirement about data integrity limited to the data needed to interpret raw data (Metadata). According to the requirements regarding full disclosure, ref. [II], any relevant data generated in a company in relation to a given product, drug or device, falls under the requirements for data integrity.

Reported in ref. [III], the following key definitions by FDA regarding data are stated:

Data integrity (FDA):

For the purposes of this guidance, data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate

Metadata (FDA):

Metadata is the contextual information required to understand data. A data value is by itself meaningless without additional information about the data. Metadata is often described as data about data. Metadata is structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data. For example, the number "23" is meaningless without metadata, such as an indication of the unit "mg." Among other things, metadata for a particular piece of data could include a date/time stamp for when the data were acquired, a user ID of the person who conducted the test or analysis that generated the data, the instrument ID used to acquire the data, audit trails, etc. Data should be maintained throughout the record's retention period with all associated metadata required to reconstruct the CGMP activity (e.g., §§ 211.188 and 211.194). The relationships between data and their metadata should be preserved in a secure and traceable manner.

In Europe Annex 11 ref. [V], was released along with an update of EudraLex chapter 4, Annex 11 includes the EMA requirements to data but no definition giving room for wide interpretations of the term data.

Data (EMA):

Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

Common for both FDA an EMA is the requirement and expectation for audit trails when dealing with data, refs [III] and [V].

Audit trail (FDA):

For purposes of this guidance, audit trail means a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. An audit trail is a chronology of the "who, what, when, and why" of a record. For example, the audit trail for a high performance liquid chromatography (HPLC) run could include the user name, date/time of the run, the integration parameters used, and details of a reprocessing, if any, including change justification for the reprocessing. Electronic audit trails include those that track creation, modification, or deletion of data *(such as processing parameters and results) and those that track actions at the record or system level (such as attempts to access the system or rename or delete a file). CGMP-compliant record-keeping practices prevent data from being lost or obscured (see §§ 211.160(a), 211.194, and 212.110(b)). Electronic record-keeping systems, which include audit trails, can full fill these CGMP requirements.*

Audit Trails (EMA)

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

Additional FDA definitions and interpretations exists in ref. [III].

These might seem logical and obvious given the widespread use of personal logins, passwords, and session logging in today's systems. But as there, so far, have not been formulated any legacy clause, unlike with 21 CFR part 11, the combined requirements and demands for data, data integrity, audit trail, and metadata also applies to equipment and old computer systems.

4 Discussion

The easiest way to discuss the generation of data to a batch report is to track the measured value from measuring point to the final report prior to printing.

When a data point is measured, on an old piece of equipment, it is typically measured as an analogous signal, which is converted to a digital signal and recorded by a PLC, either a hardware or a software PLC. The PLC then transmits the data to the computer, where the data is stored in a dedicated file. The file either contains all data in a chronological form, or the file can be dedicated to a certain type of measurements.

The data may then be displayed in an "online" trend curve, which monitors the process, Furthermore, the data also forms the basis for the batch report. However, often the unsorted data in their .txt or .csv files does not contain all of the related metadata. Often the file only contains a TAG identifying the measuring probe, and a time stamp to define it position in the data set, but rarely the unit of the given measurement, as this does not become relevant until the data point is either plotted on the trend or added to the batch report.

The individual data point remain in their respective files until the batch report is generated and they are printed in a sorted meaningful way, with all relevant metadata.

After generating the batch report the data forming the batch report remains located in separate files or databases. This "storage", voluntarily or not, of data poses a potential risk during inspections. Because the data forming the basis of batch report is often, and rightfully so considered raw data, especially when the possibility of re-printing or holding the printing of a batch report is an option. As this would mean that the raw-data theoretically might be tampered with and therefore without proper audit trail the validity of the dataset may be questioned.

This leads to the key challenge mentioned in the beginning, namely;

How can we document that our equipment meets the requirements regarding the data?

The lack of a clear answer to this question means that the data requirements form a ticking bomb under old production equipment.

One example of the problem is with batch documentation, if the batch documentation is printed and stored in hard-copy after each batch is completed, historically this would not fall under part 11 as the physical records are controlled and stored as the one and only true copy, i.e. no data is stored digital… However quite often there is the option of reprinting a batch report for a relatively short period of time this now means that data is stored on the system and that a validated audit trail must be present and that it must be evaluated frequently.

Another example is the raw-data which forms the basis for a printed batch report. Typically in old systems this data is stored in a dedicated folder or on a dedicated partition of the computer system, as this data forms the basis of a batch report the data is to be considered GxP data and as such it falls under the afore mentioned rules and regulations.

A third, example relates to user accounts. Many old systems do not allow for appropriate account security, I.e. password lengths, complexity and similar, these requirements might not be stated explicitly, however they are a logical consequence of the requirements regarding electronic signatures.

A fourth and final example are validated audit trails, or rather the lack thereof, as many old computer systems store audit trail files in easily accessible files such as .txt or .csv, files which, as mentioned before, are stored in easily accessible folders.

In general terms the solutions to the problem could be to perform either an automation or system upgrade, where the computer system, both hardware and software, will be brought into the 21st century, or to simply scrap the old equipment and buy new modern equipment. Both of these solutions are time consuming, and they both mean a significant investment in equipment, which most likely produces a product that is almost, if not already, off patent, meaning little incentive to make major investments in the process. This is possibly why many choose another third solution, a solution which is in fact very popular to "solve" the challenge of new requirements. This solution is to write rationales-.

Rationales that states either why the equipment is in compliance, or which is often the case, why the system does not need to be in compliance, or rather does not need to meet the requirements while staying in compliance.

5 Conclusion

As a consultant and engineer responsible for or participating in the upgrade or re-validation of existing equipment or the qualification and succeeding validation of new it is of the outmost importance to keep in mind the issue of data integrity, as many corporations do not necessarily have this in mind when the define a task or a project.

6 References

I. Data – Merriam-Webster dictionary – www.merriam-webster.com/dictionary/data
Accessed 2016.10.04

II. Webinar FDA's increasing focus on Data Integrity – Hunton and Williams – https://www.youtube.com/watch?v=QVXcpBDAV7Q
Accessed 2016.10.05

III. Data Integrity and Compliance With CGMP Guidance for Industry – FDA – www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm495891.pdf
Accessed 2016.10.04

IV. Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application – FDA – www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm125125.pdf
Accessed 2016.10.04

V. Annex 11: Computerised systems – European Commission –

http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf Accessed 2016.10.05

6.1 Additional reading and information

Apart from the references I consider the following interesting reading on the topic:

http://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf

John Lee on data integrity:

https://www.youtube.com/watch?v=U84ujzE4Elo

MHRA on data integrity

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412735/Data_integrity_definitions_and_guidance_v2.pdf

7 Authors

- Philippe Holt – Pholt@nalys-group.com

This white paper is an attempt to summarise the issue of data and data integrity, the WP is based on released guidelines, webinars and the experience with issues from working with old equipment. It is not to be considered the official policy from any authorities.