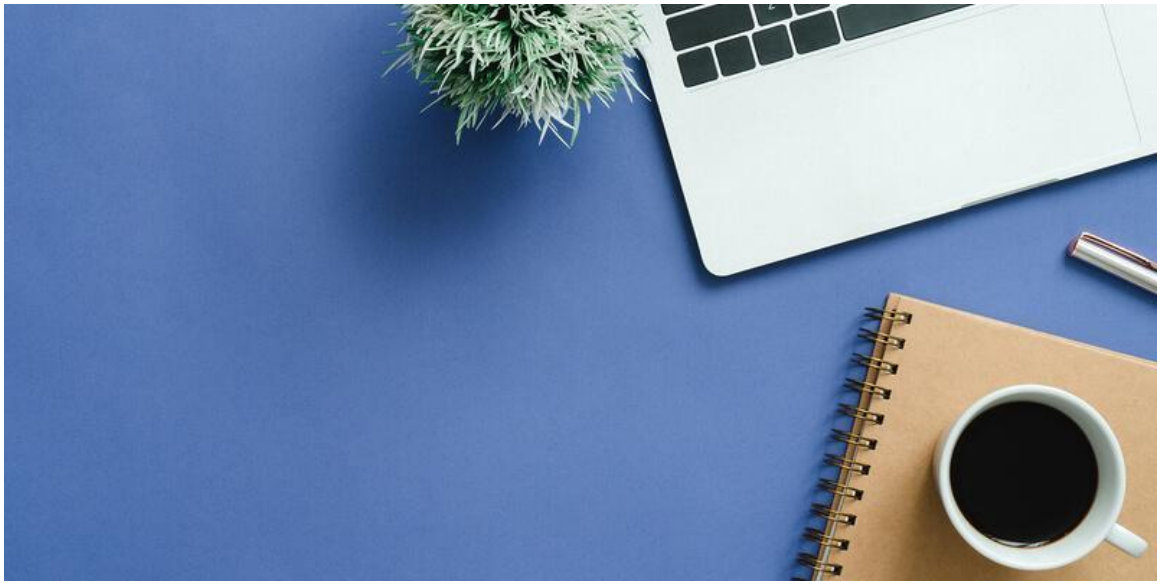
SOFTWARE TOOL VALIDATION IN THE MEDICAL DEVICE INDUSTRY

A WHITEPAPER ON REGULATORY REQUIREMENTS AND BEST PRACTICES

By:
Matteo Gubellini MScEng
&
Mirell Krain MA

CONTENTS



INTRODUCTION

Modern medical device regulations are putting more and more emphasis on the software tools that are used for development of the medical devices and can have an impact to the quality of the final product.

This whitepaper covers the requirements for validating these software tools that are not part of the medical devices themselves but support the development lifecycle of the medical device.

Nowadays companies use dozens of applications ranging from CRM and accounting tools to electronic document archives and software compilers. Most of them have no impact on the medical device.

So which ones should a medical device manufacturer validate, why and how to do it?

WHAT IS VALIDATION?

The term “validation” can have different meanings when applied to different items or in different domains.

For validation of software tools in the medical device industry, the following definitions apply.

- ***Validation*** means confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use can be consistently fulfilled. [FDA 21 CFR 820.3 (z)]

- ***Process validation*** means establishing by objective evidence that a process consistently produces a result or product meeting its predetermined specifications. [FDA 21 CFR 820.3 (z)(1)]

or in plain words, **validation is a demonstration that the software reliably does what it is supposed to do**.

WHY VALIDATE?

THE REGULATORY FRAMEWORK FOR MEDICAL DEVICE MANUFACTURERS

The requirement for medical device manufacturers to validate software tools can be found in several international standards, FDA regulations and guidance documents.

In 2022 the FDA[8] issued 538 warning letters (483s) to medical device companies, of which about 20% (105) were for process validation and 3% (17) specifically for software tool validation.

1. **ISO 13485:2016**
    a. **4.1.6**: *"The organisation shall document procedures for the* ***validation of the application of computer software used in the quality management system****. Such software applications shall be validated prior to initial use and, as appropriate, after changes to such software or its application. The specific approach and activities associated with the software validation and revalidation shall be proportionate to the risk associated with the use of the software. Records of such activities shall be maintained"*
    b. **7.5.6** Validation of processes for production and service provision: *"[…] The organisation shall document procedures for the* ***validation of the application of computer software used production and service provision****. Such software applications shall be validated prior to initial use and, as*

appropriate, after changes to such software or its application. The specific approach and activities associated with the software validation and revalidation shall be proportionate to the risk associated with the use of the software, including the effect on the ability of the product to conform to specifications. Records of the results and conclusions of validation and necessary actions from the validation shall be maintained."

2. **FDA 21 CFR 820.75** – Process Validation: *"(a) Where the results of a process cannot be fully verified by subsequent inspection and test, the process shall be validated with a high degree of assurance and approved according to established procedures. The validation activities and results, including the date and signature of the individual(s) approving the validation and where appropriate the major equipment validated, shall be documented. […]"*

In addition, specific requirements for electronic records and electronic signatures are described in **FDA 21 CFR 11** (Electronic Records; Electronic Signatures): **Subpart B** – Electronic Records, **§ 11.10** Controls for closed systems. *"[…] (a)* ***Validation of systems*** *to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."*

Detailed **guidance documents** have been developed by the **FDA** to provide recommendations and suggestions on the possible approach:

1. **General Principles of Software Validation – Final Guidance;**
2. **Guidance on Computer Software Assurance for Production and Quality System Software** (September 2022 Draft). For a detailed look into the draft guidance, please continue reading here;
3. **Process Validation: General Principles and Practices.**

WHAT SHOULD BE VALIDATED?

In the majority of cases, especially in regards to the off-the-shelf software tools, the user sees them only as black boxes. Setting up a comprehensive validation for a software tool without having an idea of its internal mechanism is a challenging task; not because of what you know, but because of what you don't. It is difficult to develop tests for unknown boundaries and unclear algorithms. And this may result in significant gaps in the validation coverage.

Recently, more mature software tool development companies have started providing **pre-validated software** and validation packages aimed at the medical device market. This is a priceless product for a medical company of any size, as it allows to demonstrate compliance using the expertise and knowledge of the developer(s) of the tool; due to their knowledge of the internal processes of the tool, they can put together a relatively lean protocol that adequately challenges the product. It also shows that the software tool developer has an idea about the regulatory framework of the medical device market, which may also help them design software tools that capture the key requirements of

the medical regulations but little known to the outside world (e.g. electronic records, electronic signatures, etc.).

A word of caution: it is best practice (as well as expected by regulatory bodies) to **repeat at least part of the validation protocol in-house**, to confirm the results of the pre-validation provided by the developer. It is unlikely that you will be able to adequately control your software tool providers (read: audit them) to be able to solely rely on their own internal activities.

Here are some general guidelines for determining the frequency of software tool validation:

1. Initial validation: The software tool should be validated before it is put into use to ensure that it meets its intended purpose and regulatory requirements.
2. Periodic validation: Software tools should be validated periodically to ensure that they continue to meet their intended use and comply with regulatory requirements. The frequency of periodic validation depends on the criticality of the use of the software tool and the risk associated with its use.
3. Changes to the software tool: Whenever changes are made to the software tool, such as upgrades or modifications, the software tool should be revalidated to ensure that it continues to meet its intended use and regulatory requirements. The frequency of revalidation depends on the extent and impact of the changes made.
4. Change in use: If the intended use of the software tool changes, the software tool should be revalidated to ensure that it is still suitable for its new use. The frequency of revalidation depends on the extent and impact of the change in use.
5. Regulatory requirements: Regulatory requirements may specify the frequency of software tool validation. For example, some regulations require annual validation of software tools used in critical processes.

Post-validation activities

Validation is not limited to an activity at a certain point in time. A company must ensure that a software tool remains validated during its use until its retirement. In other words, you will need to conduct validation regularly.

1. **Periodic Review**: it is good practice to periodically review the validation status to ensure that the activities and conclusions are still valid.
2. **Change Management**: you will have to reassess the software after changes have been implemented.

Example from Industry

Q: What type of activities are required for validating an external software tool?

A: These three types of activities can be leveraged for validation:

1. Testing is probably the bulk of the activities. Make sure you include appropriate corner cases.
2. Quality Assurance activities can also support the validation effort, e.g. periodic backups (and backup validation), procedures detailing access control, appropriate training of users, etc.
3. Documentation provided by the software tool developers.

HOW TO VALIDATE?

APPROACH TO VALIDATION

STEP 1 – Create an Inventory List

It is extremely useful to begin by **creating a list of all the software tools and their functionalities that are in use in the organization and define their intended use**, e.g. are they used for accounting, personnel management, product development or for the electronic Quality Management System.

STEP 2 – Assess the Impact

Once you have the full list of software tools, you should **assess the impact of** each of these **tools on the medical device(s)** you are developing.

If a software tool has an **impact on the "quality" of the device** (in the broader sense), then validation may be required. Consider also that the software tools used to manage your Quality System documents, including CAPAs, complaints, NCs, requirements, risks, etc., fall into this category.

The FDA Guidance "Computer Software Assurance for Production and Quality System Software" provides several examples of assessment of software tools.

STEP 3 – Define Validation Framework

The **framework for the software tool validation** mimics the well-known steps used for process validation:

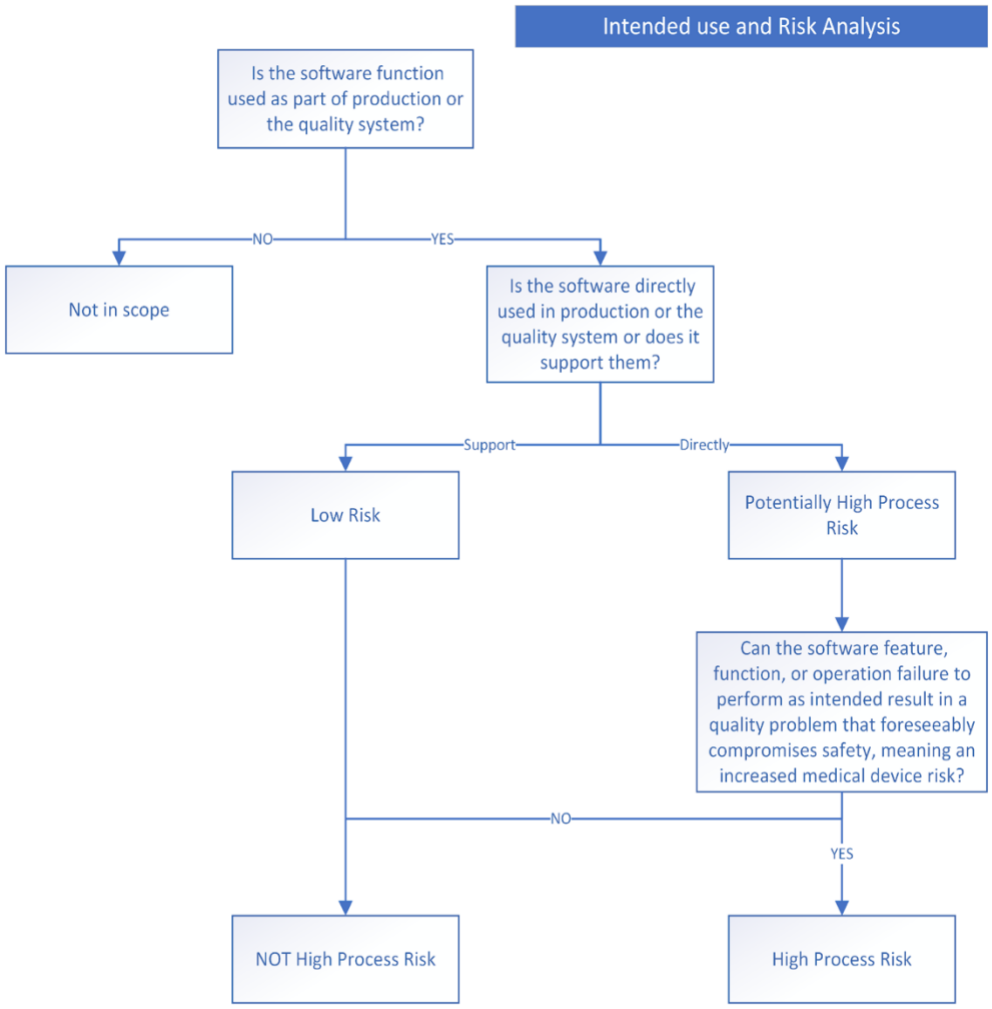
1. Create and document a validation plan: scope, approach, resources, schedules and the types and extent of activities, tasks, and work items.[1]
2. Carry out a risk assessment, as discussed above;
3. Document requirements identification, including the intended use and the features in scope;
4. Create a validation protocol, to cover all requirements and intended use, and trace to them;
5. Record validation results: pass, fail, evidence, deviations and anomalies;
6. Summarize everything in a validation report. A summary of the activities completed and any relevant note.

FDA recently released a draft guidance document on Software Tools Validation that we have summarized in a flowchart below and that you can follow in validating your software tools.

As indicated in the flowchart below, it is useful to break down your software package into "functions". Software typically has a number of different features with varying degree of importance to your application.

To define the scope of the validation, consider the following questions:

1. What features of the software will be used (for production or Quality System)?
2. Of those, which ones have an impact on quality?
3. Of those, which ones are more critical?



This first screening will help you narrow down the **scope of your validation** effort and identify features that need more thorough validation.

STEP 4 – Complete and Record Validation Activities

To complete the validation, you need to record and approve your validation results.

This is usually presented in the format of Validation Report filled with documented evidence on the tests run during validation. You should capture if the results were as expected or if there were any deviations. Based on the report you can assess if the results are acceptable or if you need to correct some features before continuing to use the software tool.

Example from Industry

Q: What features of Atlassian Confluence Cloud should I validate?

A: Define the features of Confluence that you are using. Confluence has hundreds of features but only a handful of them might be used for regulated activities you're your Document Management System, e.g. Page Management; Permission Management, Data Retention and Integrity.

When validating Confluence Cloud, you should focus on key features such as user access controls, data backups and recovery, integration with other tools, document management, collaboration and communication, and compliance with regulatory requirements. By validating these features, you can ensure that Confluence Cloud meets its intended purpose and complies with regulatory requirements.

Below is a fragment of a risk assessment for a cloud software tool as an example that lists the functionality that the tool is used for, its impact on the Quality, Risk Score and validation method and regularity to be followed:

Software Tool Inventory			RISK ASSESSMENT			Additional details about the Tool	Validation approach		
Software Tool	Functionality used / Intended use	Impact on Produc Quality (YES/NO) if not functioning the way expected?	Severity	Probability	Risk Level	Hosted on	Validation regularity	Methodology	Resources
Confluence	*Page management*	*Yes*	*High*	*Medium*	*High Process Risk*	*Cloud*	*Regular*	*Automated testing*	*Validation for Confluence app*
	Document retention		*High*	*Medium*	*High Process Risk*				
	Permission management		*High*	*Medium*	*High Process Risk*				
	Data integrity		*High*	*Medium*	*High Process Risk*				
	Team brainstorming		N/A	N/A	Not in scope		*N/A*	*N/A*	*N/A*

Q: What are the most critical features of Confluence Cloud?

A: For Document Management in Confluence Cloud, data integrity is probably the most important, followed by permission management and electronic signatures.

VALIDATION OF CLOUD SOFTWARE TOOLS

While validating a software tool that is not fully under your control is difficult enough, the situation is even more complicated when the software tool resides on the cloud and is controlled by the tool developer. This is a scenario that will become more and more frequent due to the popularity of Cloud and SaaS tools.

Main Characteristics of Cloud software tools:

1. They are managed by external organizations;
2. Changes to the software happen regularly and incrementally, with a little or no notification to the users;
3. Users cannot opt-out of changes to the software, e.g. security patches.

The characteristics of the Cloud software tools impose a series of challenges to their users, especially if they are from the regulated industries.

Possible Challenges of using Cloud Software tools:

1. Software tool developers might not know about the MedTech regulatory requirements and may not be eager to meet them as they cater also to other industries (that have less requirements);
2. Audits of the software provider may not be possible at all;

3. Unexpected and “uncontrolled” changes may happen to the software tools with no notice provided to the users.

Approach to Validating the Dynamic Cloud tools

Medical device manufacturers have always been skeptical about dynamic Cloud tools as they are not in full control of them. At the same time, using Cloud tools, in many cases you can enjoy better service with advanced security and low(er) maintenance costs.

Most medical device manufacturers try not to update the software tools they have implemented as the re-validation effort is substantial. This does not bode well with security patches that need to be implemented immediately - 0-day vulnerabilities are extremely dangerous and there is no day that goes by without news of known software tools being attacked with new vulnerabilities being exploited.

Repeating the whole validation manually every week is not realistic - not even part of it can be done at periodic intervals fast enough before new updates are released.

That’s where software tool developers can help with their insights. Features like “integrity checkers”, “self-validators”, “status reports”, etc. can provide the necessary evidence that the initial validation is still valid and that the tool is still running as expected.

Example from Industry

Q: How are changes implemented and communicated to users of Atlassian Confluence Cloud?

A: Atlassian makes changes to Confluence Cloud each day. Unfortunately, the users are not informed about the different types of changes made, which means that a regular validation of your Confluence Cloud instance is the best way to see if it is working as expected. Manual validation of Confluence Cloud takes 2 man-weeks at the minimum.

Quality Assurance of Cloud Software Tools

Several solutions are available to ensure the continued validity of the initial validation of the software tools.

Testing is only one of the activities a medical device manufacturer as an end-user can select for this purpose, e.g.:

- Unscripted testing, such as:
    - Ad-hoc testing
    - Error-guessing
    - Exploratory testing
- Scripted testing
    - Robust scripted testing
    - Limited scripted testing

AUTOMATED VALIDATION

Due to the frequent changes in Cloud software tools, manual validation will not be able to keep up with them. This is where automated validation is required.

Automated validation should be run regularly to check the integrity of your Cloud software tool.

Example from Industry

Q: How can I automatically validate my Confluence Cloud instance?

A: You can use the Validation app for Confluence Cloud to run the automated integrity checks of your Confluence instance once every 7 days. As a result of each run, you will have the validation protocol and validation results with documented evidence. Test Results describe each test that was run recording the documented evidence (the screenshots) highlighting the result (pass/fail) of the test. The Validation App supports compliance with the requirements of ISO 13485:2016 Clause 4.1.6 and FDA 21 CFR 11.

To learn more about the automated validation app for Confluence, you are welcome to **join a Webinar on Validation of Cloud tools**. Please register here.

CONCLUSIONS

Medical device manufacturers are required to validate the software tools that are used for production and their Quality System.

This White Paper describes why medical device manufacturers need to validate their software tools and how they can conduct such validation regularly. The White Paper covers the regulations that require validation and the best practices of conducting validation of Cloud Software tools that are provided by external organizations of which the users have no control over.

The White Paper also provides practical insight from industry, in particular on validating Atlassian Confluence Cloud in the case where a medical device manufacturer uses it for their Document Management System.

REFERENCES

1. ISO 13485:2016 Medical devices – Quality management systems – Requirements for regulatory purposes, Clause 4.1.6, 2016
2. FDA 21 CFR 820 Section 820.75 Process Validation, https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?fr=820.75, January 2023
3. FDA 21 CFR 820 Part 11 Electronic Records; Electronic Signatures https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11, January 2023
4. FDA General Principles of Software Validation, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation, January 2022
5. Computer Software Assurance for Production and Quality System Software Draft Guidance, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/computer-software-assurance-production-and-quality-system-software September 2022
6. Process Validation: General Principles and Practices, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/process-validation-general-principles-and-practices, January 2011
7. What is Software Tool Validation?, https://softcomply.com/what-is-software-tool-validation/ , January 2019
8. FDA Inspection Observations data sheets, https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/inspection-references/inspection-observations, November 2022
9. FDA General Principles of Software Validation, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation, January 2002