AAMI

Advancing Safety in Health Technology

AAMI Consensus Report

Appropriate Use of Public Cloud Computing for Quality Systems and Medical Devices

AAMI/CR510:2021

Appropriate use of public cloud computing for quality systems and medical devices

Abstract: The purpose of this document is to provide guidance to multiple stakeholders regarding the appropriate use of public cloud computing both as a component of medical devices and in support of quality systems. Cloud technology providers, medical device manufacturers, regulatory professionals and regulators alike should be able to refer to this document to identify known best practices for ensuring that the public cloud computing component of any medical device (or quality system) works both within the spirit and the letter of regulations designed to ensure that medical devices improve patient outcomes and/or help manage healthcare costs, while also being safe and effective.

Keywords: cloud technology, cloud computing, medical devices, regulation, public cloud computing, quality systems, best practices, Software as a Medical Device (SaMD), DevOps

AAMI Consensus Report

A Consensus Report (CR) is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) developed to provide concise, prompt, and practical guidance on narrowly focused topics of high importance to the health technology community. A Consensus Report is intended to provide initial consensus guidance in response to an urgent/immediate need for guidance in the following instances:

- While more robust data/information develops on emergent areas;
- When variation in the development, implementation or use of a product or process exists;
- When existing standards or other documents require additional context/clarification.

A CR is not subject to the same formal process as a standard and while similar in nature to a technical information report (TIR), a CR is based on the collective knowledge and experience of a selected group of stakeholders and has not undergone the wider reviews of a TIR or standard and offers an even greater response time.

CAUTION NOTICE: This AAMI CR may be revised or withdrawn at any time. Because it addresses a rapidly evolving field or technology, readers are cautioned to ensure that they have also considered information that may be more recent than this document.

All standards, technical information reports, consensus reports and other types of technical documents developed by AAMI are voluntary, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Comments on this consensus reports report are invited and should be sent to AAMI, Attn: Standards Department, 901 N. Glebe Rd, Suite 300, Arlington, VA 22203-1633.

Published by

AAMI
901 N. Glebe Rd., Suite 300
Arlington, VA 22203-1633
www.aami.org

Printed in the United States of America

ISBN 978-1-57020-822-5

Contents

Page

Task Group representation

Association for the Advancement of Medical Instrumentation

Application of Quality Systems to Medical Devices Team Members

This AAMI Consensus Report (CR) was developed by a task group under the auspices of the AAMI QM-WG01 Application of Quality Systems to Medical Devices Working Group.

The task group had the following members:

Cochairs: Pat Baird
Randy Horton

Members: Clay Anselmo, Principal Quality & Regulatory Consultant, Shriner & Associates
Mike Attili, President, Amaxo
Pat Baird, Head of Global Software Standards, Philips
Randy Horton, VP Solutions & Partnerships, Orthogonal
Bernhard Kappe, CEO, Orthogonal
Artiom Kisselev, Master's student, Program in Translational Medicine, University of California Berkeley and University of California San Francisco
Josh Schulman, SVP of Clinical Innovation, MaxQ AI
Nicola Zaccheddu, Sr. Software Quality Engineer, Philips

NOTE Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

Acknowledgements

Application of Quality Systems to Medical Devices Team members would like to thank the many people who took time, energy, and brainware to help us talk through ideas, give feedback, and provide insights based on their own work. Some have asked to remain anonymous, and we thank you; you know who you are. We offer thanks to:

Sharon Cholowsky, Arterys
Maria D'Azevedo, The Experien Group
Rich DeLaCruz, Silver Lake Group
Beko Jang, Arterys
Nigel Lambert, Komodo Cloud
Zian Liu,The Experien Group
Michael (Moose) O'Donnell, Program in Translational Medicine, University of California Berkeley and University of California San Francisco
Jessica Richter, The Experien Group
Torin Taerum, Arterys

Introduction

Cloud computing's rapid growth in this century is a story of the incredible power of economies of scale and the ways that applying that economic principle to the provisioning of server-side computing has had tremendous benefits in terms of cost, reliability, security, agility, and functionality. When compared to other computing platforms, one of the key strengths of cloud environments in general, and public cloud environments[1] specifically, is that they constitute a platform where changes and updates can be frequently, rapidly, and widely deployed. Changes may include, for example, the addition of more computing power in the form of additional servers or the adaptation of the environment to protect against cybersecurity threats.

This allows for effective continuous change and integration cycles where minor changes are rolled out to users, but the user does not have visibility into the type and extent of testing performed by the public cloud vendor prior to deployment. While cloud providers retain the capability to rollback these changes if issues are encountered, any rollback decisions are in the cloud provider's hands and not their customers' control. While Service Level Agreements (SLAs) can help in this domain, public cloud providers today have not generally demonstrated a willingness or ability to provide rollback as a feature or an option in any SLAs.

For medical devices and quality systems, the benefits of public cloud computing come with a new set of risks. In gaining access to the value of the public cloud, manufacturers give up a degree of control, including change management, over the computing platform. The common paradigm for performing verification and validation rests on the concept that the platform and environment are static between programmed releases, which are re-validated focusing on the changes and their potential impact on other parts of the system. For the last three decades, the key methods the medical device industry has used to ensure device safety and performance have been planning, evaluating, controlling, and validating all changes to the device and its operating environment prior to deployment.

Running in the cloud breaks the paradigm of being able to maintain a validated state by initiating validation when there is a change to the environment. In the cloud, the computing environment is abstracted to the point that one may not know when there is a change to hardware or software, and therefore not know precisely when to initiate validation. While SLAs can help in this domain, due to the fundamental nature of the cloud computing model and the current economics of public cloud computing, any SLA-based approach to this issue might not be a comprehensive solution. Often the manufacturer is not given the means to verify and to accept or reject a change before it is applied to the system. In some cases, that information is simply unavailable before the change occurs. In other cases, a change notification may be available but contains only a high-level summary of changes and perhaps tests performed. The traditional idea of a continuously validated state is simply not possible.

As a result, classic change management, which is one of the core processes that underlies the lifecycle of regulated medical devices, is difficult to apply considering the requirements specified in the 21 CFR 820:30, 21 CFR 820:70(i) and ISO 13485:2016. This presents a real-time challenge to maintaining the validated

[1] For the purposes of brevity, when this Consensus Report refers to cloud computing, it is specifically addressing public cloud computing using the NIST SP800-145 definition: "The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."

However, the same points may be relevant for non-public cloud computing as defined in this same NIST publication: private, hybrid, and community.

state of a medical device and the software tools used to develop and support them. The degree of this challenge is directly proportional to the degree of change control delegated to the cloud service provider.

There are clear requirements in nearly all global device regulatory frameworks that medical devices and software support tools are verified and validated prior to deployment and that changes that could affect the operation/safety of the device or tool are assessed and revalidated, as necessary. These requirements apply regardless of the selected computing environment. Depending on the level of sensitivity of a device or tool to various types of changes, unknown or uncontrolled changes may cause the functionality to change in unintended and unapproved ways, possibly impacting safety or performance. As a result of the ongoing, real-time changes associated with the cloud environment, maintenance of a validated state is a significant challenge.

Under these conditions, the best that can be achieved is an intermittently validated state.

It is worth noting that these conditions have some analogy in design validation and verification of medical device performance. One common way is through the use of scheduled, periodic verifications of the entire device. This can be combined with ongoing proactive monitoring to confirm that the underlying technologies enabling the device are functioning as specified. (See Recommendation 3 later in this CR for further discussion of the exact frequency of ongoing quality control checks.) It is also worth noting that this is not the only circumstance where you do not have complete visibility into software or environment changes: Wi-Fi, cellular, internet connectivity, and to some extent, mobile hardware and operating systems may be outside the manufacturer's direct control and changes may not be visible.

Regulators have consistently promulgated a risk-based approach to verification and validation, both in terms of testing depth and documentation. Consistent with this as an overlay to verification and validation in the cloud environment, risk mitigation becomes key to reducing the risk that changes to the computing environment between validation will affect the device or tool in an adverse way.

It is the consensus of the Application of Quality Systems to Medical Devices Team members that in many cases achieving an intermittently validated state with a high benefit/risk ratio is acceptable, provided that medical device manufacturers understand and plan for the changes that may occur in real-time on commercial cloud platforms and respond in an educated, thoughtful, and responsible manner to address the corresponding risk and ensure continued effectiveness and safety.

To take advantage of the benefits of the cloud environment, without unidentified and unmitigated risk, requires an extension of typical risk analysis and risk control practices to analyze external dependencies and associated potential failure modes more fully.

Risk Analysis specific to cloud computing should focus on:

- what changes can occur between validations;
- how likely it is that each change will impact safety or effectiveness;
- what can be done to detect those changes;
- how long will it take to correct or mitigate them; and
- what harms could occur before correction or mitigation.

Server-based computing risks typically center around data or service availability or data corruption and the processes or functions that depend on these. Where there is a high safety risk in "real time" that cannot be addressed through design and where mitigations cannot be implemented prior to an adverse event, these functions should not be "in the cloud."

Ultimately a benefit-risk analysis is necessary to understand the advantages of the cloud environment on performance, scalability, simplicity, and security, versus the potential risks of the chosen cloud service model along with feasible risk mitigations.