INTEROPERABILITY STANDARDS AND RISKS, MEDICAL DEVICE SAFETY

Konstantinos Makrodimitris, PhD

US FDA/DHHS

FDA DISCLAIMER

The views and opinions presented here represent those of the speaker and should not be considered to represent advice or guidance on behalf of the U.S. Food and Drug Administration.

INTEROPERABILITY STANDARDS AND RISKS, MEDICAL DEVICE SAFETY

- Interoperability standards to help us control risks for medical device
- The right measure(standard) to improve interoperability for the right patient, time, place,
- SDC 11073 standards and device safety clauses
- Examples (open discussion), ISO14971, IEEC62304
- Categories : Medical devices, EHR, MDDS, Mobile apps,

Interoperability Guidance(2016)

Contains Nonbinding Recommendations

Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on: September 6, 2017

Manufacturers' risk analysis should consider the risks associated with interoperability, reasonably foreseeable misuse, and reasonably foreseeable combinations of events that could result in a hazardous situation. Based upon these risks, a manufacturer may want to change the design of the device, the intended interoperability scenarios, or include device limitations and/or warnings to reduce risks to acceptable levels. As discussed in ISO 14971, risk control measures may not be necessary for risks that are broadly acceptable;[8] these decisions should be captured within the risk analysis documentation.

FDA emphasizes that the same process of defining hazardous situations, risks, and mitigations can be used when considering a system that contains more than one connected medical device. There may be additional hazardous situations that arise in these conditions. The manufacturer should specify which mitigations are implemented and which are necessary for safe use but may require implementation by other parties, such as the party responsible for set-up or installation. These should be included in the risk analysis section of the submission.

For devices subject to the risk analysis in 21 CFR 820.30(g), FDA recommends including an analysis of the interface or interfaces on the devices, the intended connections, and any effects that the connection may have on the device performance. The normal risk analysis submitted should include hazards that were considered, possible hazardous situations, the risks that may result from each, and how the hazards and risks were addressed. Your submitted analysis should include the normal elements in a risk analysis and address:

- the risk control measures for reducing unacceptable risks to acceptable levels;
- fault tolerant behavior, boundary conditions, and fail safe behavior such as how the device handles delays, corrupted data, data provided in the wrong format, unsynchronized or time mismatched data, and any other issues with the reception and transmission of data;
- any risks potentially arising from security vulnerabilities[9] that may be

Mobile Medical Apps (FDA 20150

Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices

---

Guidance for Industry and Food and Drug Administration Staff

Document issued on February 9, 2015.

An MDDS does not modify the data, and it does not control the functions or parameters of any connected medical device. An MDDS does not include devices intended for active patient monitoring.[3] Devices intended for active patient monitoring include the following characteristics:

- The clinical context requires a timely response (e.g. in-hospital patient monitoring).

§ 880.6310 Medical device data system. (a) Identification.

(1) A medical device data system (MDDS) is a device that is intended to provide one or more of the following uses, without controlling or altering the functions or parameters of any connected medical devices:

(i) The electronic transfer of medical device data;

(ii) The electronic storage of medical device data;

(iii) The electronic conversion of medical device data from one format to another format in accordance with a preset specification; or

(iv) The electronic display of medical device data.

(2) An MDDS may include software, electronic or electrical hardware such as a physical communications medium (including wireless hardware), modems, interfaces, and a communications protocol. This identification does not include devices intended to be used in connection with active patient monitoring.

Multiple Function Device Products: Policy and Considerations(FDA 2015)

Medical products may contain several functions, some of which are subject to FDA's regulatory oversight as medical devices, while others are not. For purposes of this guidance, for any given product, the term "function" is a distinct purpose of the product, which could be the intended use or a subset of the intended use of the product. Products with at least one device function are referred to as "multiple function device products." This draft guidance explains FDA's regulatory approach and policy for all multiple function device products. Specifically, this guidance clarifies when and how FDA intends to assess the impact of other functions that are not the subject of a premarket review on the safety and effectiveness of a device function subject to FDA review. The purpose of this draft guidance is to identify the principles, premarket review practices, and policies for FDA's regulatory assessment of such products and to provide examples of the application of these policies.

E. Requirements and Specifications

Documentation of requirements and specifications included in the premarket submission for the device function-under-review should include adequate detail to describe any expected relationship, utility, reliance, or interoperability with any other function. For example, the

B. Does the Impact Result in Increased Risk or Have an Adverse Effect on Performance?

If the other function impacts the device function-under-review, the extent of the impact should be evaluated. Although the inclusion of other functions in a product may impact the device function-under-review, the assessment should focus on identifying if there may be increased risk and/or an adverse effect on performance due to the *combination* of the other function with the device function-under-review.

1. Impacts to Safety

A risk-based assessment should be used to identify and analyze all risks of a device function-under-review, including those that may result from the inclusion of other functions in the product. If the impact results in no increased risk, then no additional risk mitigation is necessary. If there may be increased risk, then the risk should be appropriately mitigated, and the appropriate verification and/or validation should be performed to ensure the effectiveness of the mitigation. The following examples can be used as a guide to understand increased risk.

SaMD risk/algorithms/clinical

What is Software as a Medical Device?

The term Software as a Medical Device is defined by the International Medical Device Regulators Forum (IMDRF) as **"software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."**

Use of Software as a Medical Dev
platforms, including medical devic
few. Such software was previously
"standalone software," "medical d
other types of software.

- *SaMD is a medical device and includes in-*
- *SaMD is capable of running on general pu platforms.*[3]
- *"without being part of" means software nc to achieve its intended medical purpose.*
- *Software does not meet the definition of Sa hardware medical device.*
- *SaMD may be used in combination (e.g., a medical devices.*
- *SaMD may be interfaced with other medic devices and other SaMD software, as well*
- *Mobile apps that meet the definition above*

in a larger system.

7.2 SaMD Categories

State of Healthcare situation or condition	Significance of information provided by SaMD to healthcare decision		
	Treat or diagnose	Drive clinical management	Inform clinical management
Critical	IV	III	II
Serious	III	II	I
Non-serious	II	I	I

7.3 Criteria for Determining SaMD Category

Criteria for Category IV –

i. SaMD that provides information to treat or diagnose a disease or conditions in a critical situation or condition is a Category IV and is considered to be of very high impact.

Criteria for Category III –

i. SaMD that provides information to treat or diagnose a disease or conditions in a serious situation or condition is a Category III and is considered to be of high impact.

http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf

SaMD risk/algorithms/clinical

- Analytical (Accuracy, Reliability, precision)
- Clinical validation (Sensitivity, Specificity)

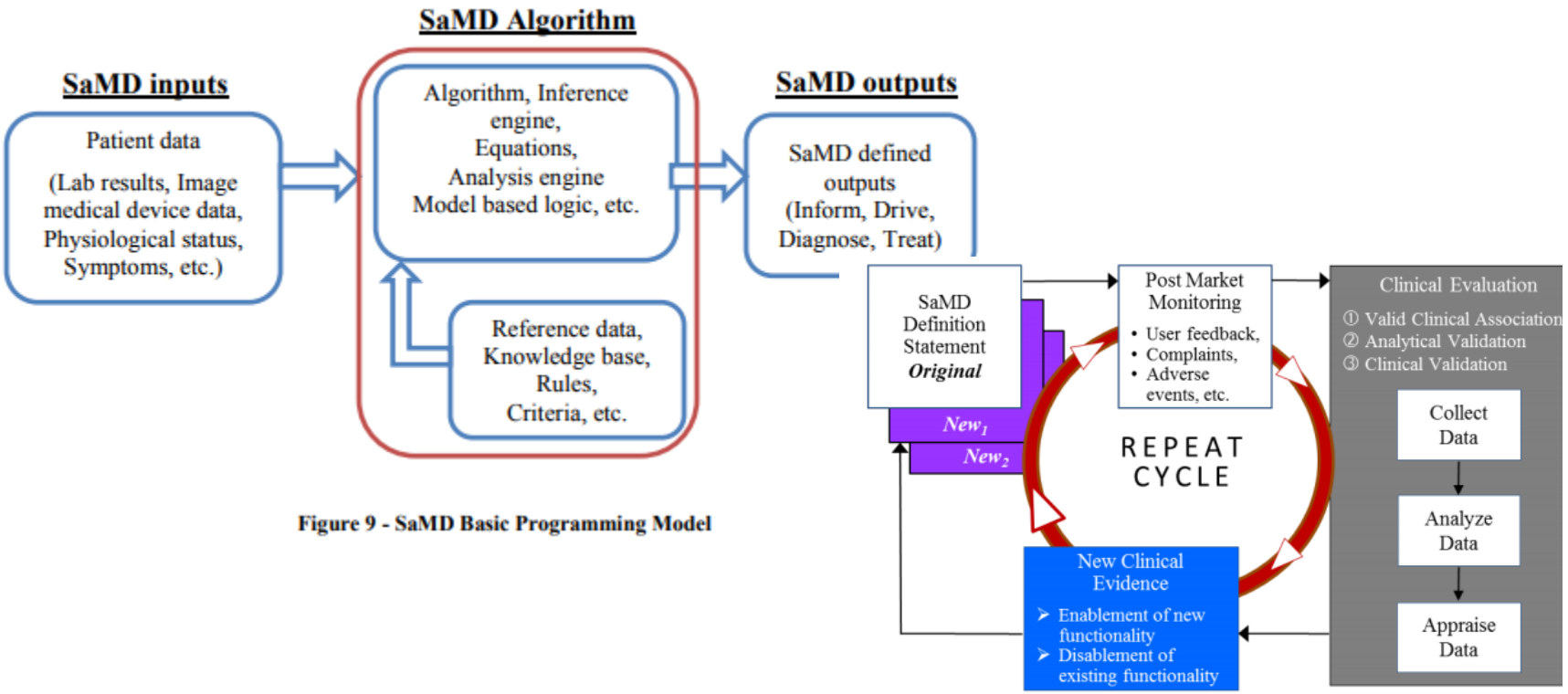

Figure 9 - SaMD Basic Programming Model

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm524904.pdf

QUESTIONS/DISCUSSION

- Project to gather specific material on interoperability standards addressing safety and risks (examples, clauses, categories,)
- White paper 2019-2020 to publish and disseminate for comments
- Introduce LOINC/SHIELD/SNOMED, interoperability in vitro diagnostic devices and assays (Mike Waters, FDA)

Cybersecurity Guidance(2016)

Postmarket Management of Cybersecurity in Medical Devices

Manufacturers should define, as part of the comprehensive cybersecurity risk management, the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria. These steps allow manufacturers to triage vulnerabilities for remediation (see Section VI for additional information on risk assessments).

Threat modeling is important in understanding and assessing the exploitability of a device vulnerability and potential for patient harm. Threat modeling can also be used in determining whether a proposed or implemented remediation can provide assurance that the risk of patient harm due to a cybersecurity vulnerability is reasonably controlled. Importantly, acceptable mitigations will vary depending upon the severity of patient harm that may result from exploitation of a vulnerability affecting the device. For example, a cybersecurity vulnerability affecting the temperature reading of a thermometer may have different risks than a cybersecurity vulnerability affecting the dosage of an insulin infusion pump because of the severity of patient harm.

VI. Medical Device Cybersecurity Risk Management

As part of their risk management process consistent with 21 CFR part 820, a manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, est
evaluating the associated risks, controlling these risks, and monitoring the eff
controls. This process should include risk analysis, risk evaluation, risk contr

Figure – Evaluation of Risk of Patient Harm. The figure shows the relationship between exploitability and severity of patient harm, and can be used to assess the risk of patient harm from a cybersecurity vulnerability. The figure can be used to categorize the risk of patient harm as controlled or uncontrolled.

Thank you