Questions and Answers for an Application of Registration and Market Approval to Cybersecurity in Mobile Medical Devices

March 2022

I. Introduction

In order to help the medical device manufacturers understand the requirements for premarket review of mobile medical devices in Taiwan, this Q&A is specially prepared in conjunction with the " Cybersecurity Risk Assessment Report for Medical Device" published by the Taiwan Food and Drug Administration of the Ministry of Health and Welfare on December 6, 2021. This document assists the manufacturers to solve common problems when evaluating the cybersecurity of medical devices and finalizing the evaluation report. However, with the rapid development of cybersecurity technology, the manufacturers shall still properly implement the cybersecurity evaluation of the medical devices according to the product and technical characteristics.

II. Questions and Answers

Q1:

If Bluetooth-enabled medical devices are paired and bonded by Bluetooth low energy (BLE) between the devices, in such a manner that only the bonded devices are able to receive and read data, do they comply with the cybersecurity requirements?

A1:

In accordance with the essential principles from the “Guidance for Industry on Management of Cybersecurity in Medical Devices”, the medical device manufacturers shall maintain the products’ confidentiality and integrity. Any kind of pairing/bonding technology could be recognized as an authorization. If the data can only be accessed under authorization, this is consistent with cybersecurity requirements. In brief, no matter which security technology was used, the cybersecurity risks can be assessed in accordance with the “Guidance for Industry on Management of Cybersecurity in Medical Devices” and the “Cybersecurity Risk Assessment Report for Medical Device”.

Q2:

If the data generated from the medical device can be accessed by the third-party apps, is it considered as a violation of cybersecurity according to the “Guidance for Industry on Management of Cybersecurity in Medical Devices”?

A2:

If the access has been authorized, and comply with the essential principles from the “Guidance for Industry on Management of Cybersecurity in Medical Devices”, the access may not be seen as a violation.

Q3:

Could a self-defined data format for data transmission be regarded as one kind of data encryption? If the transferred file from the medical device is encrypted as the data cannot be read without special software or the profile format is proprietary, does it comply with cybersecurity requirements?

A3:

In accordance with the essential principles from the “Guidance for Industry on Management of Cybersecurity in Medical Devices”, the medical device manufacturers shall maintain the products’ confidentiality and integrity. The evaluation of cybersecurity risk and hazardous situation for algorithm or profile applied for data encryption should be considered comprehensively. If a self-defined data format could be a kind of data encryption and the evaluated residue risks were acceptable, a self-defined data format could be considered to comply with the products’ confidentiality and integrity of the cybersecurity requirements. In brief, no matter which security technology was used, the cybersecurity risks can be assessed in accordance with the “Guidance for Industry on Management of Cybersecurity in Medical Devices” and the “Cybersecurity Risk Assessment Report for Medical Device”.

Q4:

Before completing the medical device cybersecurity assessment report, do the relevant risk assessment documents need to be done firstly? For example, when assessing the type of data transmitted by the system, if the data are damaged or stolen, what kinds of risk events would happen and how to evaluate its’ control methods?

A4:

Yes, as mentioned in the “Cybersecurity Risk Assessment Report for Medical Device” section 3.1.1 “Security Requirement Specification and

Threat Modeling”, the first part is the identification of assets refers to the important assets in the medical device project, such as personal user data, algorithms, and other related features. Whether the data are transmitted internally or externally, all belong to the category of important assets. The second part is the data flow diagram (DFD), which should depict reliance intervals and reliance boundaries to demonstrate the flow of products’ data and its controllable range. After that, the relevant cyber risks can be identified, as stated in section 3.3 “Analyzing Cyber Security Threats”, each of the identified assets is analyzed for possible threats and listed in the threat list.

Q5:

Can the vulnerability assessment be tested by a third-party laboratory or the manufacturer solely?

A5:

Vulnerability assessment can be tested based on product characteristics and Cybersecurity Risk Assessment results, and it can be done by sending the product to a third-party laboratory for testing or some manufacturers have cybersecurity-related departments with certified testers who conduct the testing by themselves. The circumstances depend on the manufacturers.

Q6:

Regarding the” Cybersecurity Risk Assessment Report for Medical Device” in section 2.2 “Security Requirement Specifications”, under what circumstances should be filled in No or Not Applicable for each item in the checklist?

A6:

This section is to be completed by the manufacturer according to the internal design of the product at the time of development. For example, when asking whether using an encryption mechanism for sensitive data transmission or not, fill in Yes if the manufacturer has used such a mechanism; if not, fill in No. If the questions that do not apply to the product should be marked Not Applicable. For example, when considering the input data validation based on the obtained information from external devices, in the case that the system did not request the external data, it should be filled in Not Applicable.

Q7:

If the corresponding answer for an item in the cybersecurity requirement checklist is No, do we still need to include the SRS for this item?

A7:

If a particular item does not apply to the manufacturer's product and is not considered to be a risk, the manufacturers do not need to include an SRS. When the application is reviewed, however, it will be considered whether the item poses a risk; given that answers are provided through self-disclosure, if the manufacturers consider a particular scenario to be a potential risk, then an SRS will later need to be implemented to address this risk.

Q8:

According to one item in the third section of the Cybersecurity Requirements Checklist, we must assess whether the product "Uses a publicly available, internationally verified and unhacked algorithm"; Does cloud transport SSL satisfy this definition?

A8:

The algorithms to use and the level of encryption are at the manufacturer's discretion and will be reviewed and adjusted afterward based on whether the residual risk is acceptable in the risk assessment for medical device cybersecurity.

Q9:

Article 5 of the Cybersecurity Requirements Checklist instructs, "Do not use self-created encryption"; if a manufacturer uses a self-created encryption method, are they required to verify the strength of the encryption?

A9:

The manufacturers shall maintain the confidentiality and integrity of their own medical devices to comply with cybersecurity requirements; Even if the manufacturers use self-created encryption, the cybersecurity shall be assessed comprehensively and the residual risk should be acceptable with the verification of the encryption. No matter which security technology was used, the cybersecurity risks can be assessed in accordance with the " Guidance for Industry on Management of Cybersecurity in Medical Devices" and the " Cybersecurity Risk Assessment Report for Medical Device ".

Q10:

What are the configuration management items in the Cybersecurity Requirements Checklist?

A10:

This refers to the software or device’s config file. For example, the file could be hardware or software settings when executing the software or devices, such as AI parameters or OS configuration files.

Q11:

Can the contents of Security Requirement Specification (SRS) and Security Detail Design (SDD) be the same?

A11:

The SDD is how the manufacturers actually achieves SRS when designing products. Multiple SDDs may correspond to one SRS, however the content could be the same or not, depending on the cybersecurity requirements.

Q12:

What kinds of contents can be filled in as proof in the test result of the Security Validation & Verification (SVV)?

A12:

The pictures, test results, quote attachments (excerpt vulnerability scanning, for example) could be included in the test result of the Security Validation & Verification (SVV). The manufacturers should declare whether Pass or Fail of the test results in the SVV table.

Q13:

For the “Cybersecurity Risk Assessment Report for Medical Device” section on threat modeling, is there an established international standard for its evaluation or can it be evaluated on its own?

A13:

Threat modeling can be evaluated by taking international organization standards as reference or by self-assessment. The manufacturers can also refer to Section 3.1.1 Security Requirement Specification & Threat Modeling of the " Cybersecurity Risk Assessment Report for Medical Device", including " Assets Identification", "Data Flow Diagram (DFD)" and "Cybersecurity Threat Analysis ".

Q14:

Should the Data Flow Diagram (DFD) be expanded in the case of multiple user role types?

A14:

Yes. However, if different user role types can perform the same function, you can simplify the DFD and note this information.

Q15:

Does the “Cybersecurity Risk Assessment Report for Medical Device” section “Cybersecurity Risk Assessment form” Ease of discovery and awareness (V1) refer to users or developers?

A15:

This refers to the user. The ease of discovery and awareness depends on which operating system used; for example, if the device is a mainstream device or the used operating system (OS) still supported by the OS company, the mentioned situation above could fill in score of 1. Potentially if the hackers’ willingness to attack the customization operating system is low, the manufacturer could also fill in score of 1.

Q16:

If a threat is not a high risk to users, how should we enter its risk level (Impact Factor) in the Cybersecurity Risk Assessment form?

A16:

The risk level can be indicated as 1 if the manufacturer evaluates the threat to the patients is a low risk. However, threats, such as data manipulation, may still easily occur; at this moment, the risk probability is considered as high. Therefore, this table lists the extent to which all possible cybersecurity risks could affect patients. If the review document reveals a high level of risk to patients (users) and a discrepancy with the manufacturer's assessment, the manufacturer should identify the details of the risk and develop relevant control measures to reduce it to an acceptable level.

Q17

Should the manufacturers check all the items in the “Cybersecurity Risk Assessment Report for Medical Device” section 3.4 “Cybersecurity Risk Assessment form”?

A17:

This section is completed based on the manufacturer’s identified assets and the risks which the assets may be exposed to.

Q18:

If the vulnerability and penetration test report is conducted by a third-party company, can the report be included as an attachment?

A18:

For vulnerability and penetration testing, whether the testing is conducted by an in-house team or by a third-party lab, the test report should detail concerning the testers, the items tested, the framework used to test the conditions, and the version of the testing tools used, among other factors. The report can be included as an attachment, or the report can include a brief description of which tests were passed, which lab performed the tests, and the results of the tests, with the full report attached.

Q19:

Is it possible to define the Pass/Fail criteria of vulnerability assessment by the manufacturers?

A19:

Yes, however Pass/Fail criteria need to be disclosed and should be with scientific logic. For example, “Pass” in the checklist means that the high-risk event is not present or the risk has been appropriately reduced through controlled method.

Q20:

Should the “Cybersecurity Risk Assessment Report for Medical Device” Appendix 1 “the Manufacturer Disclosure Statement for Medical Device Security” be checked in accordance with the form?

A20:

The Manufacturer Disclosure Statement for Medical Device Security (MDS2) is endorsed by the National Electrical Manufacturers Association (NEMA) and incorporates the International Electrotechnical Commission (IEC), National Institute of Standards and Technology (NIST) and other international standards’ cybersecurity requirements covered by this document. The MDS2 will help the manufacturers to evaluate the cybersecurity of their own products within international security level. Therefore, accessing the risks by using the MDS2 is recommended.

Q21:

Does the Manufacturer Disclosure Statement for Medical Device Security (MDS2) cover both hardware and software?

A21:

Yes, in order to comply all kinds of cybersecurity in medical devices, the MDS2 covers both hardware and software.

III. Reference

1. 2020.01.15, Medical Devices Act.

2. 2021.04.29, Regulations Governing Issuance of Medical Device License, Listing and Annual Declaration.

3. 2021.05.03, Guidance for Industry on Management of Cybersecurity in Medical Devices.

4. 2021.12.06, Cybersecurity Risk Assessment Report for Medical Device.