Cybersecurity Evaluation Requirements for Medical Device Product Registration and Regulatory Update

Shiu-Huei Yeh
Section Chief of the Division of Medical Devices and Cosmetics
Taiwan Food and Drug Administration

衛生福利部
食品藥物管理署
Taiwan Food and Drug Administration
http://www.fda.gov.tw/

Outline

- **Part 1: Updates of Guidance for Industry on Management of Cybersecurity in Medical Devices**
- **Part 2: Cybersecurity evaluation requirements for medical device product registration**
- **Part 3: Example - Cybersecurity Risk Assessment Report for Cloud-based Electrocardiogram Management System**

Part 1 – Updates of Announced Guidance

■ **"Guidance for Industry on Management of Cybersecurity in Medical Devices"**

-1st announced in Nov. 2019

-Revised in May 2021

→ Renew and add references.

→ Add table of design principle/review requirements

English version:
http://www.fda.gov.tw/ENG/lawContent.aspx?cid=5063&id=3331

References:

- ✓ IMDRF
- ✓ USFDA
- ✓ Health Canada
- ✓ TGA
- ✓ Saudi FDA
- ✓ ISO 14971:2007
- ✓ UL 2900 series
- ✓ ISO/IEC 27000 series
- ✓ NIST

□ Announced 4 reference templates of cybersecurity evaluation and MDS2. (Dec. 2021, Jun 2022)

- Implantable pacemaker pulse generator
- Cloud-based Electrocardiogram Management System
- Glucose test system
- Oximeter application software

Part 2

Cybersecurity evaluation requirements for medical device product registration

Principle and Scope of Cybersecurity

- Security issues:

-Resulting from cyber connection or data transmission.

-To prevents unauthorized activities diminish the function of devices and may harm patients.

Principle

To ensure the security, safety and effectiveness of medical device.

A set of cybersecurity control measures should be periodically evaluated.

Total product life cycle.

Scope

- Applicable to the **medical devices that contain software (including firmware) or programmable logic as well as software that is a medical device (including mobile applications).**

Cybersecurity and Product Life Cycle

Exploitability	Severity of Patient Harm (if exploited)				
	Negligible	Minor	Serious	Critical	Catastrophic
High					
Medium					
Low					

Cybersecurity Risk Management

- ✓ Maintenance of Security and Primary Performance
- ✓ Identification of Cybersecurity Signals
- ✓ Analysis and Assessment of Vulnerability Properties
- ✓ Execution of Risk Analysis and Threat Modeling
- ✓ Analysis of Threat Source
- ✓ Integration of Product and Threat Detection Capacity
- ✓ Assessment of Effects of all Products
- ✓ Assessment of Compensating Control
- ✓ Assessment of Risk Mitigation Measures and Residual Risks

Premarket Review Requirements

1. **Design Documentation**
2. **Risk Management Documentation**
3. **Security Testing Documentation**
4. **Traceability Matrix**
5. **Software Bill of Material (SBOM)**
6. **Labeling and Documentation**

Part 3

Example

Cybersecurity Risk Assessment Report for Cloud-based Electrocardiogram Management System

I. Introduction

II. General Requirement

III. Cybersecurity Assessment

I. Introduction

- **Document Overview**
  - Risk analysis
  - ECG management critical parts
  - SBOM
  - Security Design Development
  - Validation reports

- **Evaluation Team**

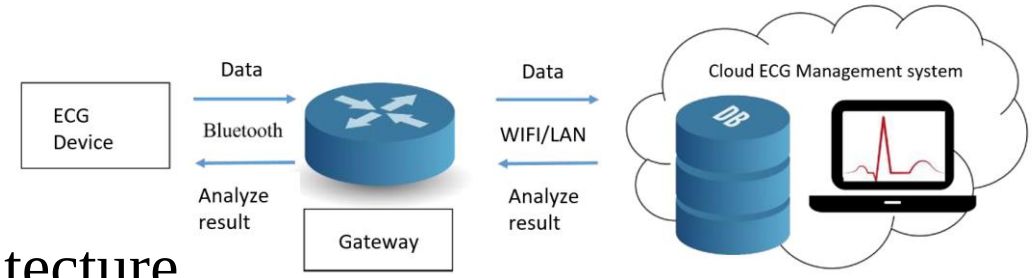
Evaluation Team
Name
Title
Specialty
Responsibility

- References

No.	Document Identifier	Title
1	ISO 14971:2019	Medical devices -- Application of risk management to medical devices
2	IEC 62304:2015	Medical device software - Software life cycle processes
3	AAMI TIR 57:2016	Principles for medical device security—Risk management
4	IEC 80001-2-8:2016	Application of risk management for IT-networks incorporating medical devices

II. General Requirement

- Development Process
  - Privacy and Security Design
  - Access Control
  - Communication Ensuring
  - Vulnerability and Update Management
  - Secure Coding Principles and Analysis
  - Vulnerability Scanning and Testing
- Intended Use



- System Operating Architecture

Account | Pairing | Data flow | Encrypted connection

II. General Requirement (continued)

- Security Requirement Specification

Category	Question	Adoption	Code
Confidentiality		Y/N/NA	
Integrity			
Availability			
Input Testing			
Authorization and Access Control			
Authentication			

- Security Detail Design
- Security Validation & Verification

II. General Requirement (continued)

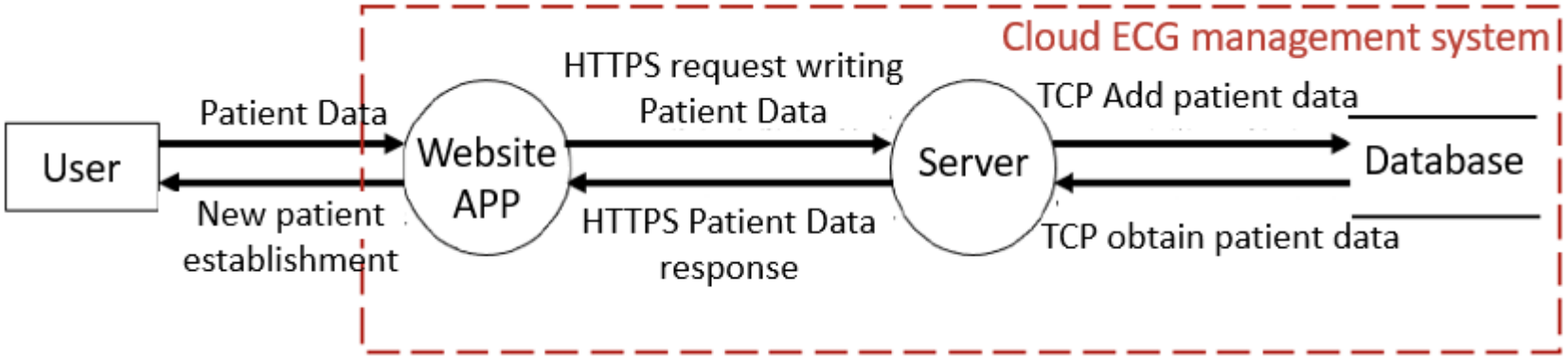
- Security Validation & Verification

Test No.	**SVV-01**
Software Version	V1.0.2
Description	The operating records of the ECG management system are properly protected and backed up to avoid unauthorized access
Operator	John
Date	2023/10/5
Method	Make sure that system logs can only be accessed by accounts with system administrative privileges
Acceptance criteria	1. account with system management authority can log in to the system, and access the system log 2. Accounts with non-administrative rights cannot log in to the system and cannot access the system logs. And system should display “Permission denied”.
Result	PASS

- Traceability Matrix

III. Cybersecurity Assessment

- Data Flow Diagram



- Cybersecurity Threat Analysis

Assets ID	Spoofing	Tampering	Repudiation	Info Disclosure	DoS	Elevation Privilege	Threat list
Operating system					V	V	D1: Shut down service or application by system hacking. E1: Elevation of privilege by creating account during hacking
System Configuration		V		V			T1: Change system function by configuration change. I1: Information disclosure by open communication interface

Manufacturer's Disclosure Statement for Medical Device Security

醫療器材網路安全之廠商揭露聲明書（Manufacturer's Disclosure Statement for Medical Device Security）

項次	細項次	主類別	項目編號	要求項目問題	符合 Yes	不符合 No	不適用 N/A	簡述符合、不符合或不適用之原因	紀錄文件
1		DOC-產品基本資料							
1.1	1	DOC-產品基本資料	DOC-1	製造商名稱	V			ABC股份有限公司	
1.2	2	DOC-產品基本資料	DOC-2	設備描述	V			雲端心電圖管理系統是一個用來收送與儲存心電圖的雲端平台	
1.3	3	DOC-產品基本資料	DOC-3	設備型號	V			雲端心電圖管理系統	
1.4	4	DOC-產品基本資料	DOC-4	文件編號	V			DOC01	
1.5	5	DOC-產品基本資料	DOC-5	製造商聯絡資訊	V			03-2118800	
1.6	6	DOC-產品基本資料	DOC-6	設備在連網環境中的預期用途	V			雲端ABC心電圖管理系統為一個封閉場域內之雲端平台，目的在於接收、儲存及顯示成人的心電圖資訊。本產品可以透過網路持續的接收從特定設備量測的單導程心電圖以及心率量測數據。醫事人員可以操作軟體，透過網路資料傳輸後檢視接收的心電圖資訊。本產品必須由擁有專業執照的醫事人員於醫療機構或照護中心使用。本系統不適合用在急重症患者身上。	
1.7	7	DOC-產品基本資料	DOC-7	文件發布日期	V			2021-11-30	
1.8	8	DOC-產品基本資料	DOC-8	協同漏洞披露：製造商是否有針對此設備的漏洞披露程序？		V		沒有針對此設備的漏洞披露程序相關文件	
1.9	9	DOC-產品基本資料	DOC-9	ISAO：製造商為情資分享和分析(ISAC)組織的會員？		V		非製造商為情資分享和分析(ISAC)組織的會員	
1.10	10	DOC-產品基本資料	DOC-10	圖表：是否有可用的網路或資料流圖來說明與其他系統元件或預期外部資源的	V			雲端心電圖管理系統網路安全評估報告	
1.11	11	DOC-產品基本資料	DOC-11	SaMD：軟體是否為醫療器材本體（即僅軟體，無硬體）？	V			軟體為醫療器材本體	
	12	DOC-產品基本資料	DOC-11.1	SaMD 是否包含作業系統？	V			本產品包含作業系統	
	13	DOC-產品基本資料	DOC-11.2	SaMD 是否依賴擁有者/運營商提供的作業系統？	V			本產品依賴擁有者/運營商提供的作業系統	
	14	DOC-產品基本資料	DOC-11.3	SaMD 是否由製造商託管？	V			本產品由製造商託管	
	15	DOC-產品基本資料	DOC-11.4	SaMD 是否由客戶託管？			V	本產品非由客戶託管	

Thanks for your attention