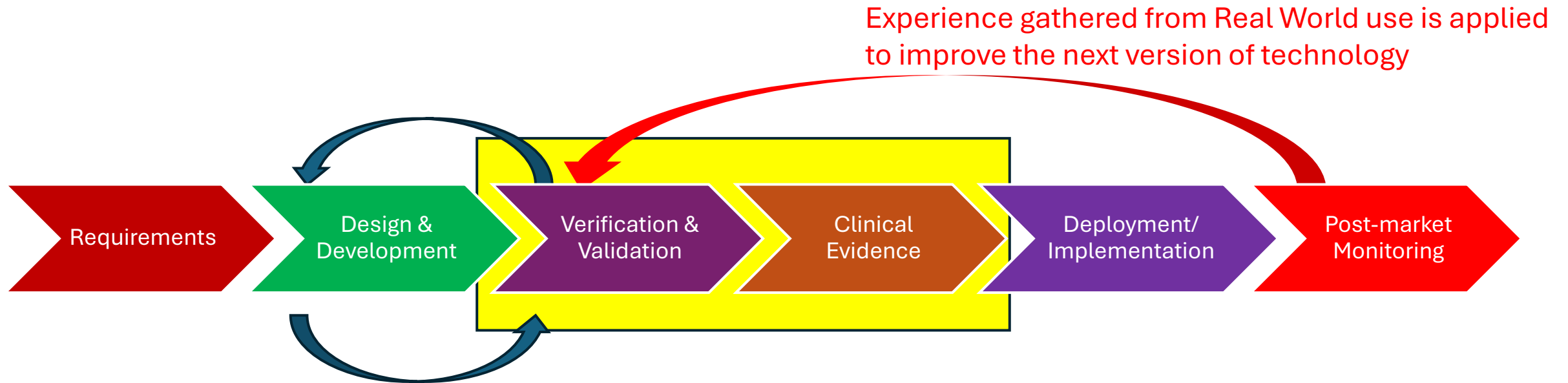


Summary of Design Verification and Validation Documents

Summary of Design Verification and Validation Documents



- เป็นข้อมูลการทวนสอบและตรวจสอบความถูกต้องของซอฟต์แวร์ รวมถึง
 - ข้อมูลที่แสดงว่าเครื่องมือแพทย์เป็นไปตามข้อกำหนดเฉพาะ (Product Spec) ของเจ้าของผลิตภัณฑ์ หรือผู้ผลิต
 - ข้อมูลที่แสดงประสิทธิภาพ และความปลอดภัย ของซอฟต์แวร์ เช่น การตรวจสอบความถูกต้องเชิงวิเคราะห์ (Analytical Validation) การตรวจสอบความถูกต้องทางคลินิก (Clinical Validation)
- เป็นข้อมูลที่จัดทำมาเพื่อสนับสนุนตาราง EP ซึ่งจะเป็นผลการทดสอบ Test Report, Validation report ตามมาตรฐานต่างๆ ที่อ้างอิงถึงใน EP เป็นต้น
- หลักฐานทางคลินิก (Clinical Evidence) ซึ่งจะเป็นรายงานการประเมินทางคลินิก (CER) พร้อมข้อมูลทางคลินิก (Clinical Data) ที่เกี่ยวข้อง

การทวนสอบและตรวจสอบความถูกต้องของซอฟต์แวร์

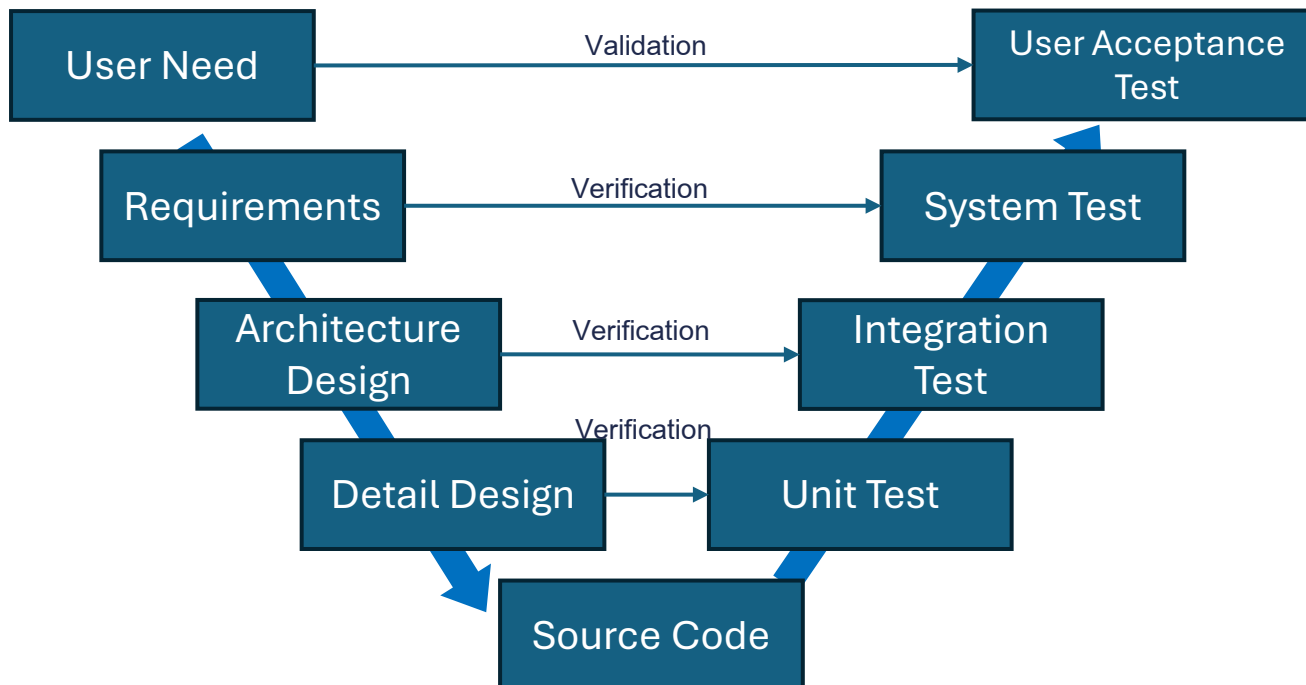
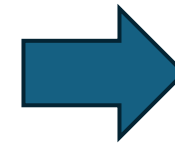
Software verification and validation

วัตถุประสงค์

Verification – ตรวจสอบว่าซอฟต์แวร์ตรงตามข้อกำหนด

Validation – ตรวจสอบว่าซอฟต์แวร์สามารถทำงานได้ตามความต้องการของผู้ใช้

วิธีการ สามารถใช้วิธีการตามข้อกำหนดของมาตรฐาน IEC 62304



Summary of Software verification and validation Report

ประกอบด้วย หมายเลขเวอร์ชันของซอฟต์แวร์ที่ทดสอบ, รายการทดสอบ, เกณฑ์การยอมรับที่กำหนด, ผลการทดสอบ, ข้อบกพร่องหรือข้อผิดพลาดที่เหลืออยู่, และสรุปการยืนยันความถูกต้องโดยรวม

IEC 62304

- 4 * General requirements
 - 4.1 * Quality management system
 - 4.2 * Risk management
 - 4.3 * Software safety classification

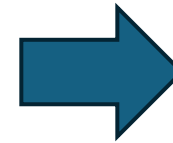
- 5 Software development PROCESS
 - 5.1 * Software development planning
 - 5.2 * Software requirements analysis
 - 5.3 * Software architectural design
 - 5.4 * Software detailed design
 - 5.5 * Software unit implementation and verification
 - 5.6 * Software integration and integration testing
 - 5.7 * Software system testing

- 6 Software maintenance process
 - 6.1 * Establish software maintenance plan
 - 6.2 * Problem and modification analysis
 - 6.3 * Modification implementation

- 7 * Software risk management process
 - 7.1 * Analysis of software contributing to hazardous situations
 - 7.2 Risk control measures
 - 7.3 Verification of risk control measures
 - 7.4 Risk management of software changes

- 8 * Software configuration management process
 - 8.1 * Configuration identification
 - 8.2 * Change control
 - 8.3 * Configuration status accounting

- 9 * Software problem resolution process
 - 9.1 Prepare problem reports
 - 9.2 Investigate the problem
 - 9.3 Advise relevant parties
 - 9.4 Use change control process
 - 9.5 Maintain records
 - 9.6 Analyse problems for trends
 - 9.7 Verify software problem resolution
 - 9.8 Test documentation contents



IEC62034 Test Report

เจ้าของผลิตภัณฑ์ จะต้องปฏิบัติตามมาตรฐาน IEC
เวอร์ชันล่าสุดและความสอดคล้องกับมาตรฐานนี้ต้องคง
อยู่ตลอดอายุการใช้งานของ SaMD (Total Product
Life Cycle - TPLC)

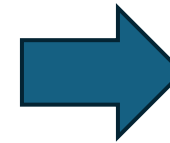
Usability Validation

วัตถุประสงค์

- เป็นการตรวจสอบซอฟต์แวร์ เพื่อให้แน่ใจว่าผลิตภัณฑ์สามารถใช้งานได้ง่าย ปลอดภัย และมีประสิทธิภาพในสภาพแวดล้อมที่กำหนด
- เป็นมาตรการลดความเสี่ยงของซอฟต์แวร์ ลดข้อผิดพลาดในการใช้งาน

วิธีการ

- ใช้หลักการเกี่ยวกับความสามารถในการใช้งาน (usability principles)
- ผู้ผลิตสามารถนำเอาวิธีการที่ระบุไว้ในมาตรฐาน IEC 62366 มาใช้กับเครื่องมือแพทย์ได้ เนื่องจากเป็นวิธีการที่เป็นที่ยอมรับ ซึ่งถูกอ้างอิงในมาตรฐานอื่นๆ



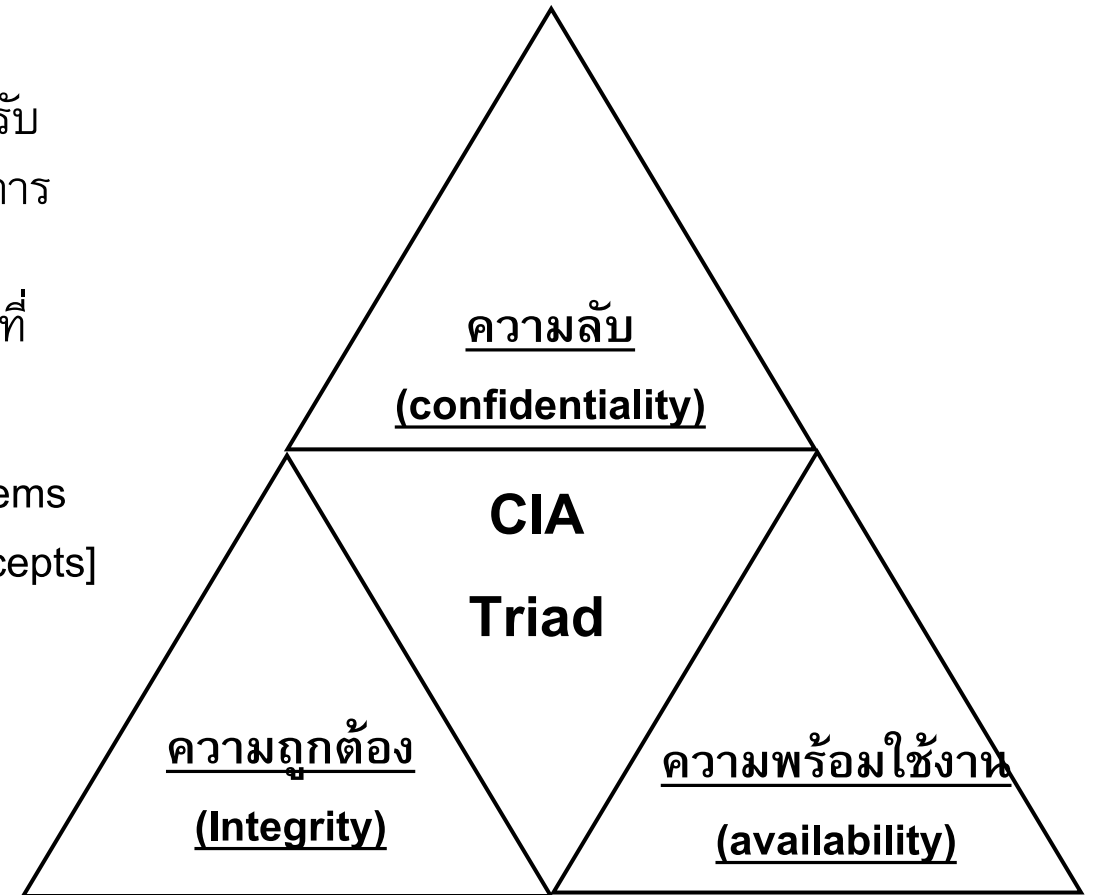
Usability Validation Report

Cybersecurity

นิยาม

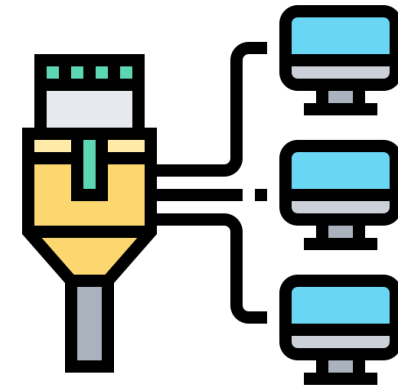
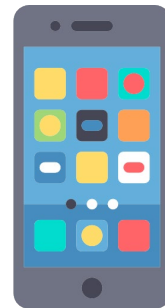
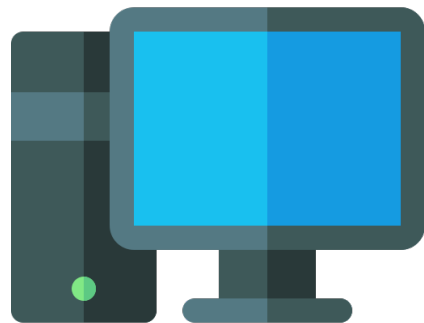
- สถานะที่ข้อมูลและระบบได้รับการป้องกันจากกิจกรรมที่ไม่ได้รับอนุญาต เช่น การเข้าถึง การใช้งาน การเปิดเผย การขัดขวาง การแก้ไข หรือการทำลาย ให้มีความเสี่ยงที่เกี่ยวข้องกับการละเมิดความลับ ความสมบูรณ์ และความพร้อมใช้งาน ที่คงอยู่ในระดับที่ยอมรับได้ ตลอดวงจรชีวิตของระบบ

[อ้างอิง ตาม ISO 81001-1 Health software and health IT systems safety, effectiveness and security Part 1: Principles and concepts]



Cybersecurity

ตัวอย่าง เครื่องมือแพทย์ที่มีความเสี่ยงด้านไซเบอร์ [เครื่องมือแพทย์ที่มีการเชื่อมต่อ]



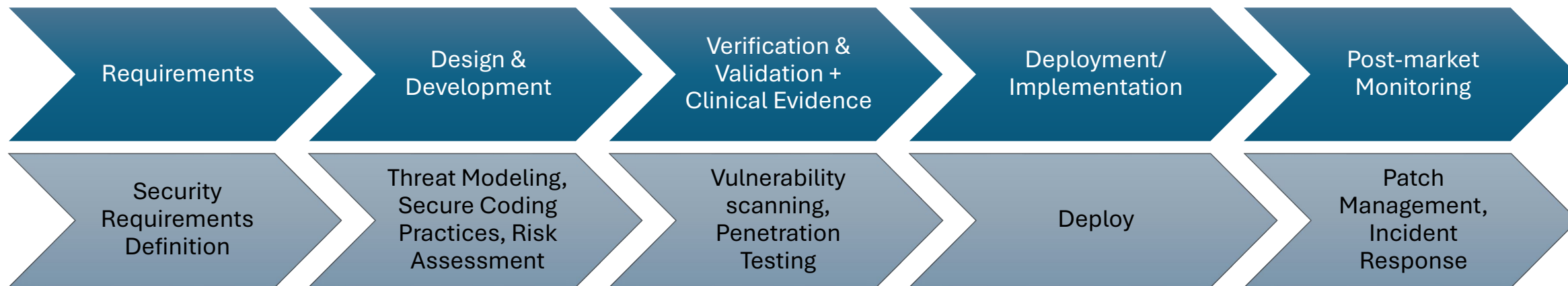
- เครื่องมือแพทย์ที่เชื่อมต่อ LAN
- เครื่องมือแพทย์ที่มีการเชื่อมต่อแบบไร้สาย: WiFi, Bluetooth Classic และ BLE (Bluetooth Low Energy)
- เครื่องมือแพทย์ที่มีการเชื่อมต่อกับอุปกรณ์คอมพิวเตอร์ทั่วไป ผ่าน USB, Bluetooth
- ซอฟต์แวร์แบบสแตนด์อโลนที่ออกแบบให้ทำงานบนอุปกรณ์คอมพิวเตอร์ทั่วไป แท็บเล็ต โทรศัพท์มือถือ, แล็ปท็อป, เดสก์ท็อป และนาฬิกาอัจฉริยะ
- ซอฟต์แวร์ที่ควบคุม ติดตามหรือส่งผลต่อการทำงานของเครื่องมือแพทย์อื่นๆ ที่เป็นฮาร์ดแวร์

Cybersecurity

ข้อกำหนดและการควบคุมด้านความปลอดภัยทางไซเบอร์สำหรับเครื่องมือแพทย์

หลักการ "ปลอดภัยตั้งแต่ออกแบบ" (safe-by-design)

ตัวอย่าง การดำเนินการด้านความปลอดภัยทางไซเบอร์ ในวงจรชีวิตของผลิตภัณฑ์ (Product Life Cycle) เพื่อให้มั่นใจว่าอุปกรณ์ทางการแพทย์มีความปลอดภัยทางไซเบอร์ตั้งแต่การพัฒนา ไปจนถึงการนำใช้ และการเฝ้าระวังหลังผลิตภัณฑ์ออกสู่ตลาด



มาตรฐานที่แนะนำเกี่ยวกับการออกแบบอุปกรณ์ให้ปลอดภัย

- IEC 81001-5-1 (not published): Health Software and health IT systems safety, effectiveness, and security – Part 5-1: Security – Activities in the product lifecycle.
- IEC/TR 60601-4-5: Medical electrical equipment – Part 4-5: Guidance and interpretation – Safety-related technical security specifications.

Cybersecurity

ข้อกำหนดและการควบคุมด้านความปลอดภัยทางไซเบอร์สำหรับเครื่องมือแพทย์

เอกสารให้ข้อมูลเกี่ยวกับความปลอดภัย (Customer Security Documentation)

ข้อมูลเหล่านี้ควรแสดงในคู่มือการใช้งาน หรือบนฉลาก หรือในเอกสารอื่นๆ

1. ข้อมูลเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น
2. คำแนะนำเกี่ยวกับวิธีการลดความเสี่ยงจากภัยคุกคามนั้น เช่น การเชื่อมต่อกับเครือข่ายที่มีการป้องกัน, การใช้โปรแกรมป้องกันไวรัส, firewall
3. ข้อกำหนดของโครงสร้างพื้นฐานที่แนะนำ
4. รายการพอร์ตเชื่อมต่อ และอินเทอร์เฟซอื่นๆ: ที่มีการรับหรือส่งข้อมูล รวมถึงคำอธิบายฟังก์ชันของพอร์ตแต่ละพอร์ตว่าเป็นขาเข้าหรือขาออก
5. ขั้นตอนการดาวน์โหลดและติดตั้งอัปเดตจากผู้ผลิต
6. ข้อมูลเกี่ยวกับการสนับสนุนหลังสิ้นสุดระยะเวลาการรับประกันแล้ว

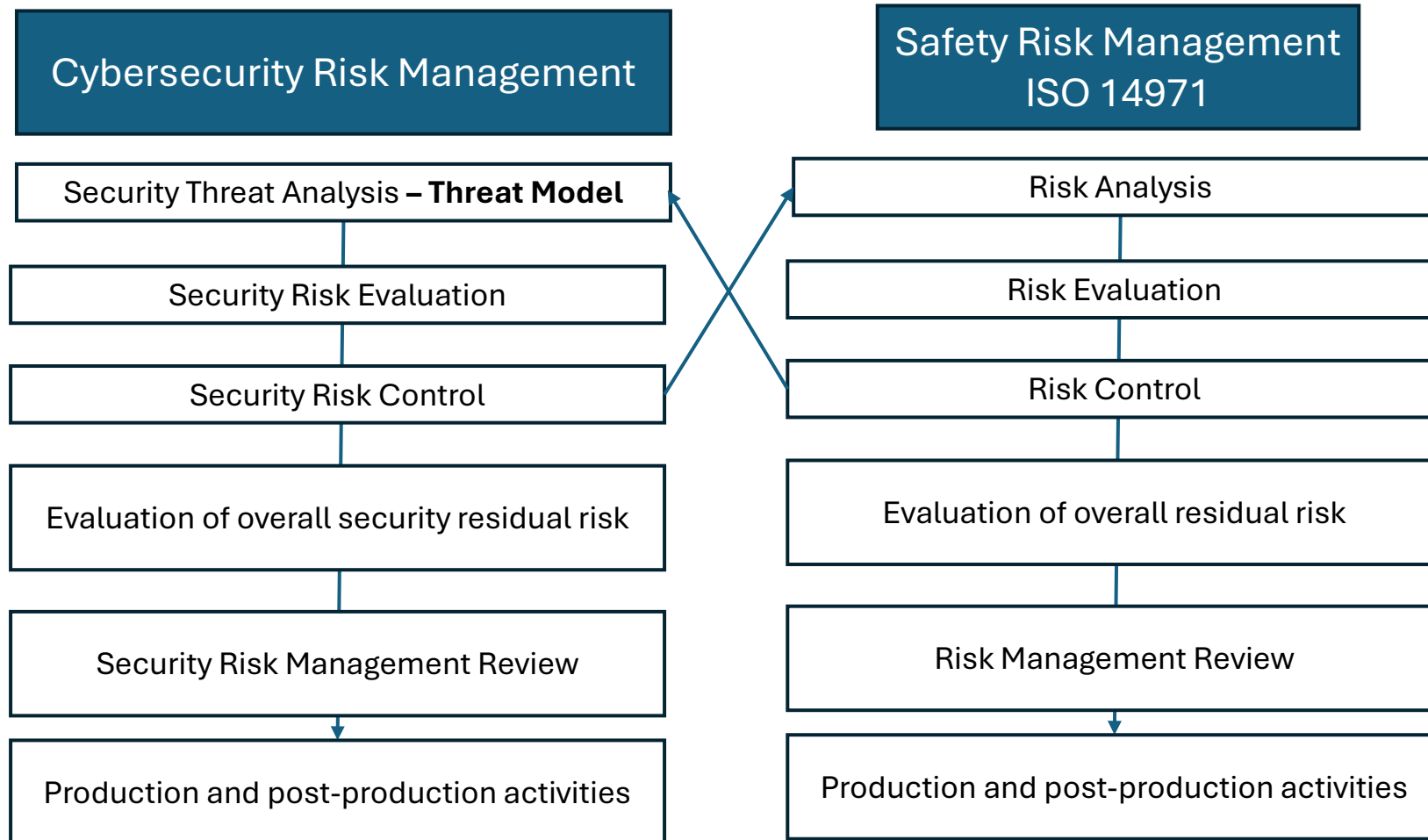
นอกจากนี้ยังรวมถึง:

- Software Bill of Materials (SBOM) คือเอกสารที่ระบุรายการของซอฟต์แวร์ที่ใช้ในระบบหรืออุปกรณ์ ซึ่งรวมถึง commercial, open source และ off-the-shelf software ที่ถูกนำมาใช้ รวมทั้งข้อมูลเวอร์ชันของแต่ละซอฟต์แวร์ด้วย SBOM มีจุดมุ่งหมายเพื่อให้ผู้ใช้สามารถจัดการกับซอฟต์แวร์ที่ซื้อมาได้อย่างมีประสิทธิภาพ และเข้าใจผลกระทบที่อาจเกิดขึ้นจากช่องโหว่หรือปัญหาที่เกิดขึ้นในซอฟต์แวร์นั้นๆ

Cybersecurity

ข้อกำหนดและการควบคุมด้านความปลอดภัยทางไซเบอร์สำหรับเครื่องมือแพทย์

หลักการในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์:



Cybersecurity

ข้อกำหนดและการควบคุมด้านความปลอดภัยทางไซเบอร์สำหรับเครื่องมือแพทย์

การทดสอบและตรวจสอบ (Verification and Validation)

หลักฐานการทดสอบหรือทวนสอบประสิทธิภาพของการใช้มาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity control measures)

- Traceability matrix ที่แสดงความสัมพันธ์ระหว่างความเสี่ยงด้านความปลอดภัย (security risks) มาตรการในการรักษาความปลอดภัย (security controls) และการทดสอบเพื่อประเมินประสิทธิภาพของการใช้มาตรการในการรักษาความปลอดภัยเหล่านั้น

Security Risk	Risk Control Measures	Verification Method	
มีผู้ไม่ประสงค์ดีเข้าถึงข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต และเข้าไปเปลี่ยนแปลงข้อมูลที่ได้จากซอฟต์แวร์ ส่งผลให้เกิดการตัดสินใจในการรักษาโดยใช้ข้อมูลที่ไม่ถูกต้อง	การล็อกอินเข้าใช้งาน ผู้ใช้ต้องยืนยันตัวตนผ่าน PIN/Password หรือ OTP ที่ใช้ได้ครั้งเดียวและมีเวลาจำกัด ข้อมูลการล็อกอินถูกจัดเก็บในเซิร์ฟเวอร์ และมีระบบตรวจสอบ	ทดสอบฟังก์ชันในการล็อกอิน ข้อมูลการล็อกอิน ถูกจัดเก็บในเซิร์ฟเวอร์อย่างถูกต้อง	Passed

นอกจากนี้ การทดสอบ ที่ควรมี

1. การหาช่องโหว่ (Vulnerability Scanner)
2. การทดสอบ หาช่องทางการเจาะระบบ (Penetration Testing)
3. การทดสอบโจมตีระบบ (DoS Attack) เพื่อรบกวนให้การทำงานของอุปกรณ์

Cybersecurity

ข้อกำหนดและการควบคุมด้านความปลอดภัยทางไซเบอร์สำหรับเครื่องมือแพทย์

การป้องกัน ตรวจสอบ และแผนรับมือกับการโจมตีไซเบอร์ต่อเครื่องมือแพทย์ [หลังออกสู่ตลาด]

การเฝ้าระวังหลังการขาย	แผนการเชิงรุกในการติดตามและระบุช่องโหว่ใหม่ ประเมินภัยคุกคาม และรับมือภัยคุกคาม
การเปิดเผยข้อมูลช่องโหว่	กระบวนการที่เป็นทางการสำหรับการรวบรวมข้อมูลจากผู้ค้นหาช่องโหว่ พัฒนากลยุทธ์บรรเทาและแก้ไข และเปิดเผยการมีอยู่ของช่องโหว่และแนวทางบรรเทาหรือแก้ไขแก่ผู้มีส่วนได้ส่วนเสีย
การแพตช์ (Patching) และการอัปเดต	แผนสรุปวิธีการอัปเดตซอฟต์แวร์เพื่อรักษาความปลอดภัยและประสิทธิภาพของอุปกรณ์อย่างต่อเนื่อง ทั้งการอัปเดตตามปกติหรือเพื่อรับมือกับช่องโหว่ที่ระบุ
การกู้คืน	แผนการกู้คืนระบบสำหรับผู้ผลิต ผู้ใช้ หรือทั้งสอง เพื่อกู้คืนระบบให้กลับมาทำงานปกติหลังจากเกิดปัญหาภัยคุกคามทางไซเบอร์

Cybersecurity

ข้อกำหนดและการควบคุมด้านความปลอดภัยทางไซเบอร์สำหรับเครื่องมือแพทย์

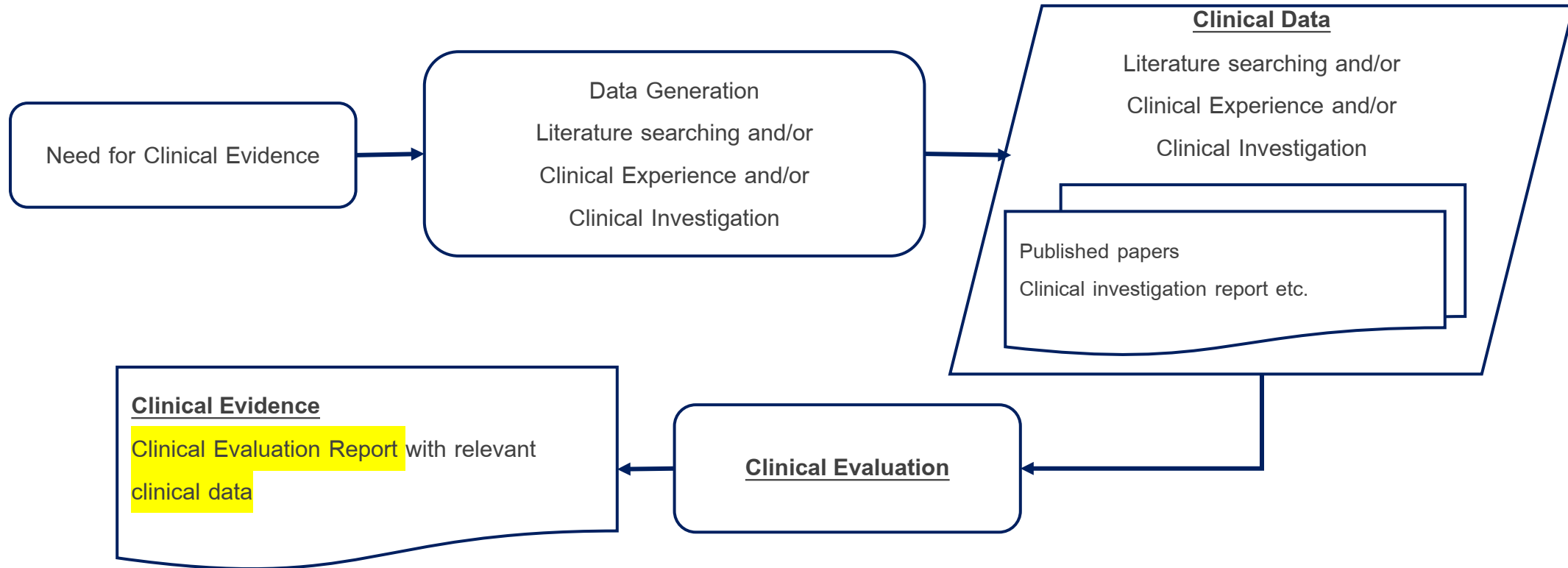
แผนการคุ้มครองข้อมูลส่วนบุคคล ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

- Data ที่จัดเก็บคืออะไรบ้าง ใครเป็น Data Controller, Data Processor, Consent เป็นต้น



Clinical Evidence

The Clinical Data and its evaluation pertaining to a medical device



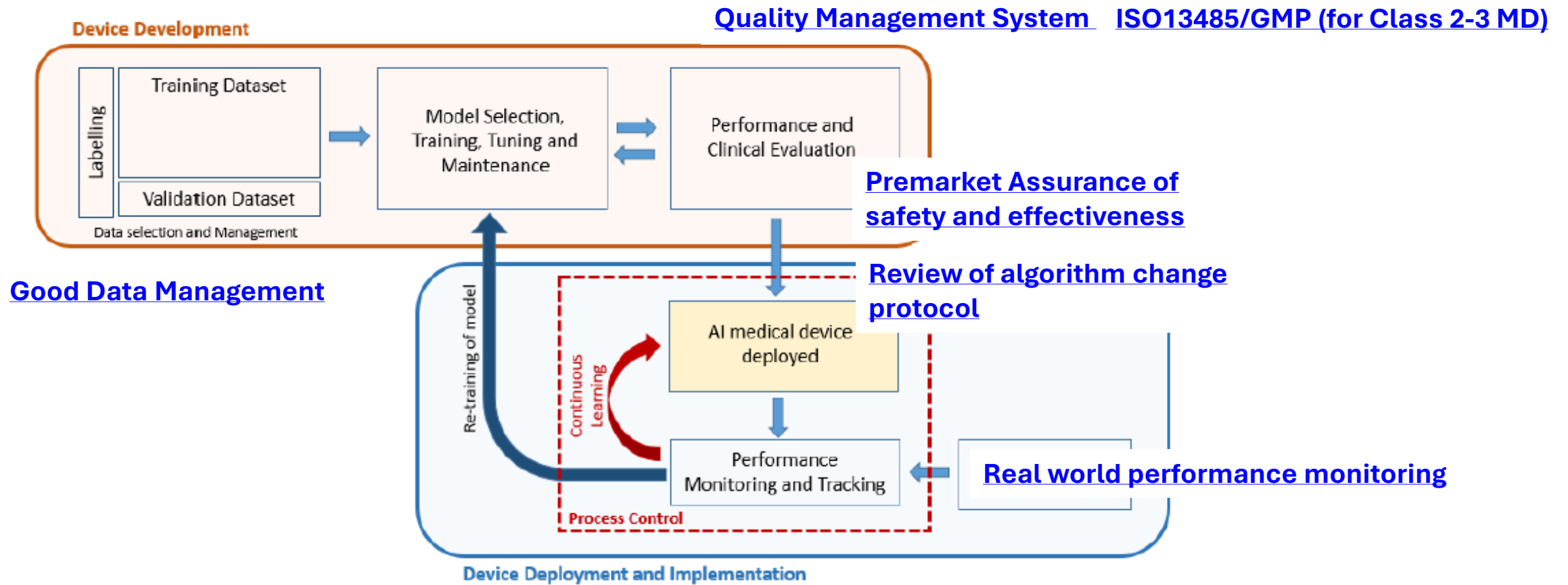
Clinical evaluation: a methodologically sound ongoing procedure to collect, appraise and analyse clinical data pertaining to a medical device and to evaluate whether there is sufficient clinical evidence to confirm compliance with relevant essential requirements for safety and performance when using the device according to the manufacturer's Instructions for Use.

Clinical Evidence

Clinical Evaluation		
Valid Clinical Association	Analytical Validation	Clinical Validation
Is there a valid clinical association between your SaMD output and your SaMD's target clinical condition?	Does your SaMD correctly process input data to generate accurate, reliable and precise output data?	Does use of your SaMD's accurate, reliable, and precise output data achieve your intended purpose in your target population in the context of clinical care?
Evidence Generation		
Use existing evidence (e.g. literature, original clinical research, etc.) or generate new evidence (e.g.. Clinical studies)	Generate evidence through verification and validation activities as part of software development process.	Generate evidence during verification and validation activities, reference existing data sources from studies conducted for the same intended use.

ข้อมูลเพิ่มเติมสำหรับการขึ้นทะเบียนเครื่องมือแพทย์ AI/ML

ภาพรวมกระบวนการพัฒนา Machine Learning



Artificial Intelligence (AI) & Machine Learning (ML)

นิยาม “locked” and “adaptive” algorithms

- Locked algorithms อัลกอริทึมที่ให้ผลลัพธ์เหมือนเดิมทุกครั้งเมื่อป้อนข้อมูลนำเข้าที่เหมือนเดิม
- Adaptive algorithm (a continuous learning algorithm) จะเปลี่ยนแปลงพฤติกรรมของตนเองโดยใช้กระบวนการเรียนรู้ที่กำหนดไว้ การปรับเปลี่ยนของอัลกอริทึมเหล่านี้จะถูกดำเนินการโดยใช้ชุดข้อมูล Input ที่กำหนด ผลลัพธ์อาจจะแตกต่างกันก่อนและหลังจากที่มีการดำเนินการปรับเปลี่ยน

[อ้างอิง US FDA]

*** เครื่องมือแพทย์ปัญญาประดิษฐ์ (AI-MEDICAL DEVICE (AI-MD)) ต้องไม่มีวัตถุประสงค์เพื่อแทนที่การตัดสินใจทางคลินิกของบุคลากรทางการแพทย์ในการวินิจฉัยทางคลินิกหรือการตัดสินใจในการรักษา ***

ข้อมูลเพิ่มเติมสำหรับการขึ้นทะเบียนเครื่องมือแพทย์ AI/ML

ข้อมูลเพิ่มเติมสำหรับการขึ้นทะเบียนเครื่องมือแพทย์ AI/ML

ข้อมูล input data	อธิบายรูปแบบของข้อมูล คุณลักษณะและเกณฑ์การเลือกของข้อมูล และกระบวนการ Pre-processing
ชุดข้อมูล (Dataset) ที่ใช้ในกระบวนการพัฒนา AI/ML	<ul style="list-style-type: none">อธิบายแหล่งที่มาของข้อมูลและขนาดของชุดข้อมูล Training, Validation และ Testing Datasetอธิบายเกี่ยวกับการ label ชุดข้อมูล การจัดการข้อมูล การใส่คำอธิบาย หรือขั้นตอนอื่น ๆ ให้ชัดเจนอธิบายเกี่ยวกับกระบวนการ Data Cleansing และการเติมข้อมูลที่ขาดหาย ต้องมีกระบวนการตรวจสอบความซ้ำซ้อนของชุดข้อมูล เพื่อให้มั่นใจว่าไม่มีการใช้ข้อมูลซ้ำซ้อนกันใน Training, Validation และ Testing Datasetให้เหตุผลถึงความเหมาะสมและความเพียงพอของชุดข้อมูลที่เลือก และปัจจัยที่อาจมีผลต่อผลลัพธ์มีการจัดการกับอคติที่เกิดจากชุดข้อมูล
ข้อมูล AI Model	<ul style="list-style-type: none">อธิบายรายละเอียดเกี่ยวกับโมเดลที่ใช้ เช่น Convolutional Neural Network - CNNให้เหตุผลที่แสดงถึงความเหมาะสมของโมเดลที่เลือก และอธิบายข้อจำกัดใด ๆ ของโมเดลพร้อมทั้งมาตรการในการลดผลกระทบจากที่เกิดข้อจำกัดเหล่านั้นอธิบายเกี่ยวกับการประเมินผลโมเดล และเมตริกที่ใช้ในการประเมินประสิทธิภาพของโมเดล (เช่น Classification Accuracy, Confusion Matrix, Logarithmic Loss, Area Under Curve - AUC) รวมถึงผลการประเมินโมเดล *การประเมินผลควรทำโดยใช้ Testing Dataset ที่แยกต่างหาก จาก Training Dataset
ข้อมูลสมรรถนะของ AI [เช่น accuracy, sensitivity, specificity]	<ul style="list-style-type: none">มีการกำหนดเกณฑ์ในการยอมรับ (Performance Criteria) หรือกำหนดคุณลักษณะด้านสมรรถนะ (Performance Specification)มีข้อมูล Test Protocol และ Test Report ในการทวนสอบและตรวจสอบว่าซอฟต์แวร์มีสมรรถนะตามที่กำหนดไว้หรือไม่มีการประเมินทางคลินิก (Clinical Evaluation)
ข้อมูล Clinical Workflow	อธิบายขั้นตอนการปฏิบัติงานที่แนะนำ สำหรับการนำผลที่ได้จากซอฟต์แวร์ไปใช้ เพื่อให้ผู้ใช้สามารถใช้งานเครื่องมือแพทย์ได้อย่างเหมาะสม รวมถึงแสดงให้เห็นระดับการมีส่วนร่วมของมนุษย์ในการใช้งาน AI
แผนการ re-training model (ถ้ามี)	มีการแสดงช่วงเวลาหรือรอบในการอัปเดตข้อมูล Training dataset ในกรณีที่มีการเก็บข้อมูลหลังจากที่นำ AI model ไปใช้งาน เพื่อนำข้อมูลนั้นใช้ใน re-training model

General Standards for Medical AI

Example of Standards Apply to SaMD

QMS

ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes

Software Life cycle

IEC 62304:2006 Medical device software — Software life cycle processes

Risk Management

ISO 14971:2019 Medical devices — Application of risk management to medical devices

Product Safety

IEC 62366-1:2015 Medical devices — Part 1: Application of usability engineering to medical devices

IEC 80001-1:2021 Application of risk management for IT-networks incorporating medical devices — Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security Part 5-1: Security — Activities in the product life cycle

IEC TR 60601-4-5:2021 Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications

IEC 82304-1:2016 Health software — Part 1: General requirements for product safety

Thank You