Digital Health US Market Pathways: Navigating an Evolving Regulatory Framework

Nikki Batista

nbatista@mcra.com

Associate Director,
Cardiovascular Regulatory Affairs

Former FDA Assistant Director in the Division of Cardiac Electrophysiology, Diagnostics, & Monitoring Devices

Highlights

- Extensive knowledge of digital health medical device regulations and policies
- Additional prior roles at FDA include Senior Lead Reviewer, Peripheral Intervention Devices Team and Lead Reviewer, Interventional Cardiology Devices Branch

Jason Tugman

jtugman@mcra.com

Associate Director,
Cybersecurity Risk Management & Strategy

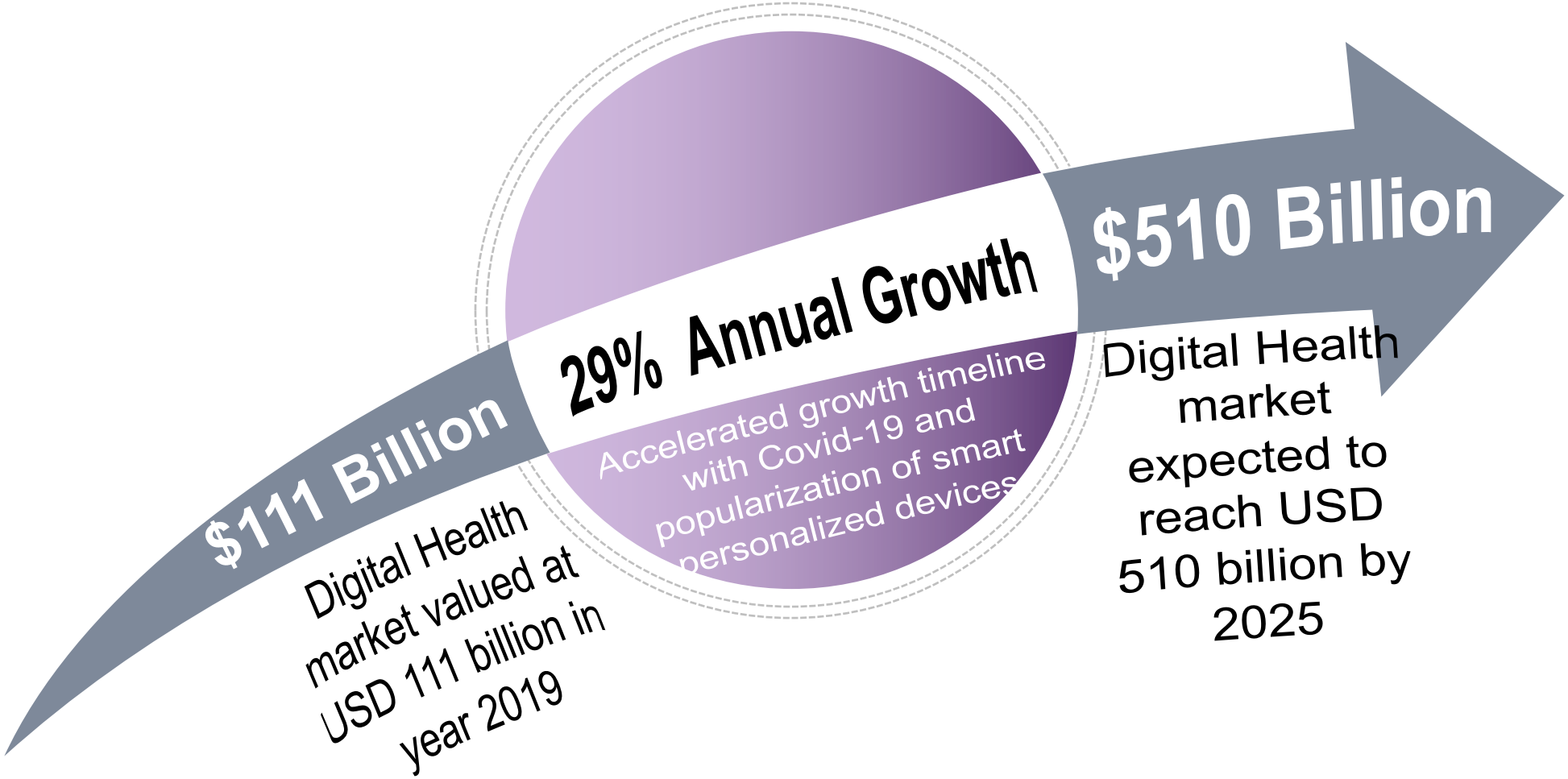
Brings 15+ years of cybersecurity experience to MCRA's Digital Health franchise

Highlights

- Extensive experience within multiple frameworks (NIST, ISO, etc.), expertise in FDA Premarket & Postmarket Medical Device Joint Security Plan (JSP)
- An active industry speaker and leader of talks regarding FDA cybersecurity in medical devices

Hello.

Rapid Market Expansion of Digital Health



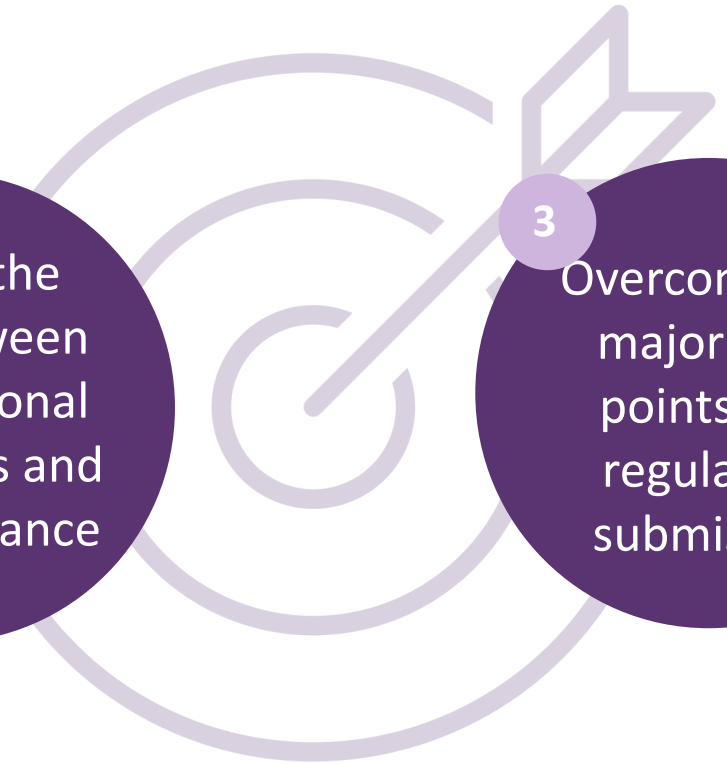
The Future of Digital Health

- Biometric monitoring permits data collection throughout our daily lives
- Big data analytics, cloud computing, and predictive algorithms will improve chronic disease management
- Hybrid of in-clinic and telemedicine expands patient-doctor interactions
- Healthcare is becoming patient-driven and decentralized
- Digital Health technologies and healthcare IT integration will be accelerated
- Cybersecurity must become a pillar of Digital Health design and innovation

41% of all 2018 cyberattacks were in healthcare sector

Today's Target

1. Determine if your technology is regulated
2. Bridge the gap between International Standards and FDA Guidance
3. Overcome the major pain points of a regulatory submission
4. Discuss the practical application of a novel regulatory paradigm



Is my technology regulated by the FDA?

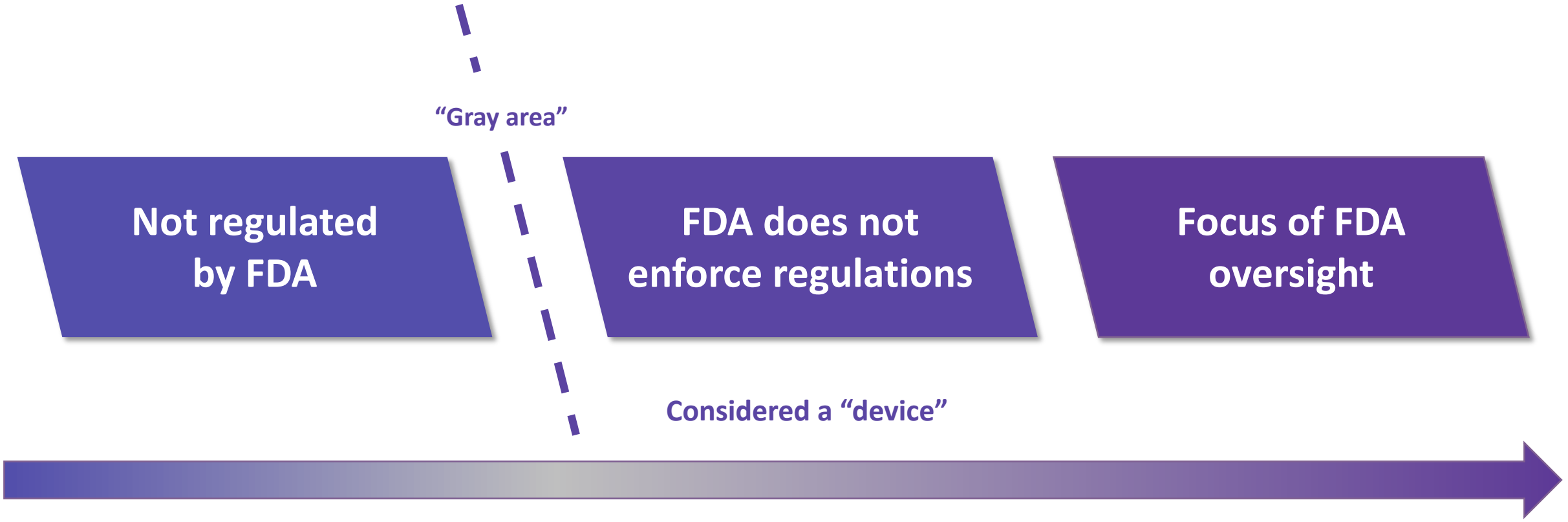
What is the level of risk associated with it?

What is its intended use?

Who is its intended user?

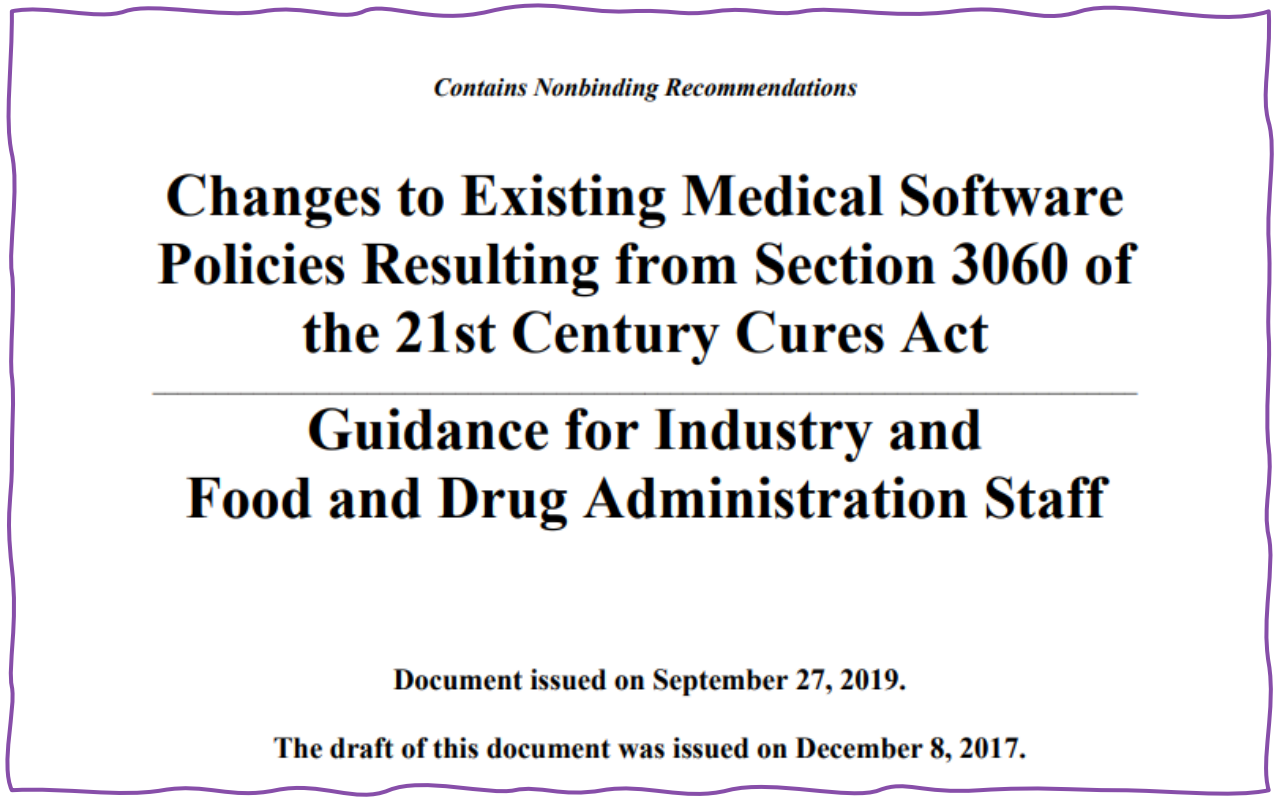
The way you market your product can determine what regulations it must follow. Remember, FDA guidelines contain broad terms and are open to interpretation, and small modifications of your product can change how it is regulated.

The Regulatory Spectrum



Is my technology a medical device?

- Does it meet the definition of a medical device per Section 201(h) of the Food, Drug & Cosmetic Act? That is – Is it intended to diagnose, cure, mitigate, treat or prevent a disease or conditions?
- Are there any aspects of your technology that are exempt from FDA regulatory oversight?



Contains Nonbinding Recommendations

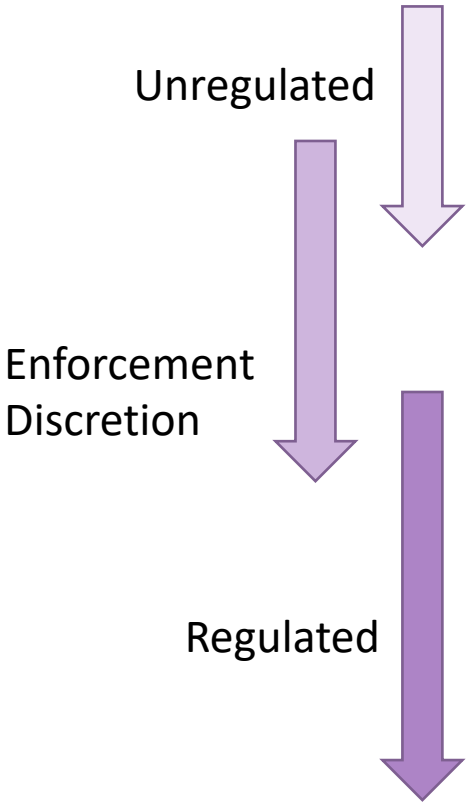
Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2019.

The draft of this document was issued on December 8, 2017.

Levels of Risk – Thermometer Example



1. “A general-purpose thermometer”
2. “This is a medical-grade thermometer”
3. “This thermometer is made for doctors to measure patient body temperature”
4. “This device takes someone’s temperature over several hours and contains algorithms that are capable of diagnosing someone with the flu.”

Where do I fall in the existing framework?

Software as Medical Device (SaMD)
- Mobile Medical Apps
- Artificial Intelligence (AL)/Machine Learning (ML) Algorithms

Wireless Medical Devices
- RFID
- Medical Telemetry

Clinical Decision Support Software
- Device CDS
- Non-Device CDS

Medical Device Data System
- Health Analytics
- Data Visualization

Telemedicine & Telehealth
- Video Conferencing
- Streaming Media
- Mobile Health (mHealth) communication

Health IT
- EHR
- Hospital Network Infrastructure

General Wellness
- Fitness and health trackers

FDA Regulated

Non-FDA Regulated

Contains Nonbinding Recommendations

Multiple Function Device Products: Policy and Considerations

Guidance for Industry and Food and Drug Administration Staff

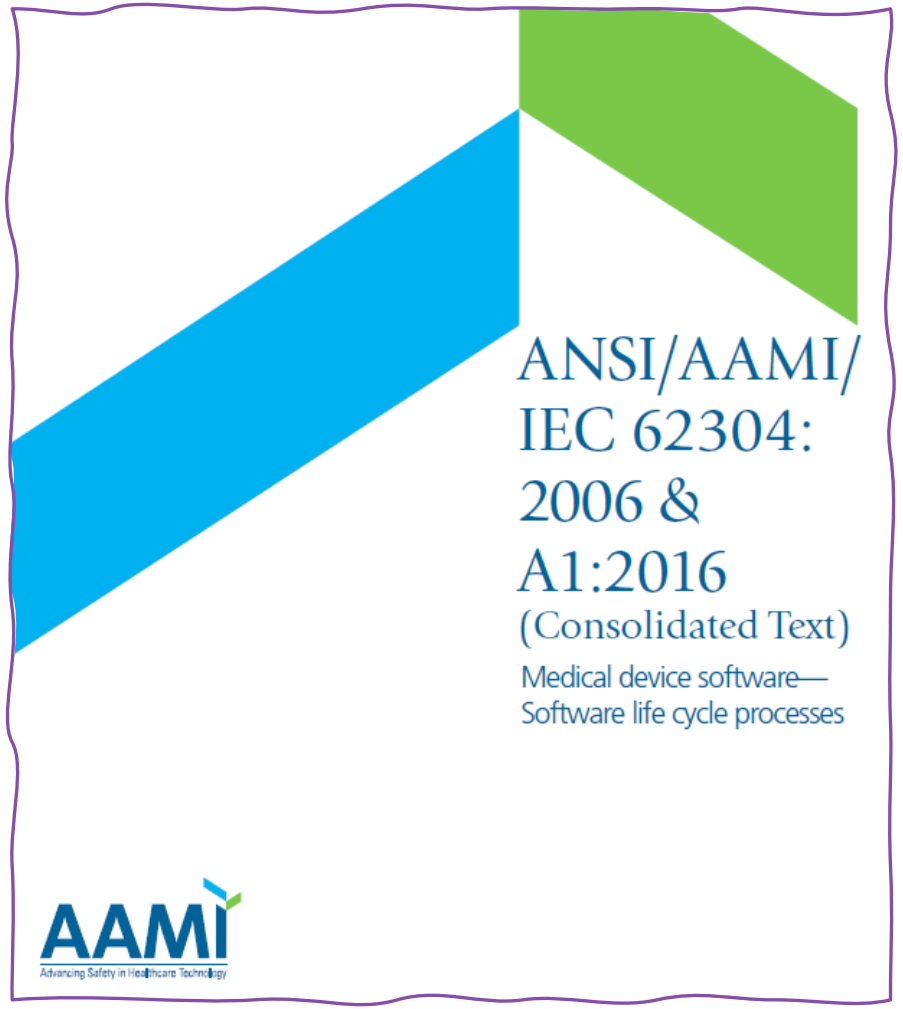
Document issued on July 29, 2020.

The draft of this document was issued on April 27, 2018.

Risk-Based Classification Systems

Class A	IEC 62304	Class C
Minor LOC	FDA	Major LOC
Class I	IMDRF	Class IV
Tier 2	Cybersecurity	Tier 1
Acceptable/Controlled	ISO 14971	Unacceptable/Uncontrolled

Your Regulatory Submission Framework



≠

Guidance for Industry and FDA Staff

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Document issued on: May 11, 2005

This document supersedes Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, issued May 29, 1998, and Reviewer Guidance for a Premarket Notification Submission for Blood Establishment Computer Software, issued January 13, 1997.

Level of Concern

Determines content of FDA premarket submission

IEC 62304		FDA
Class A	Failure or latent flaw is **unlikely to cause any injury**	Minor
Class B	Failure or latent flaw could result in **minor injury**	Moderate
Class C	Failure or latent flaw could result in **death or serious injury** to patient or operator	Major

Medical Device Cybersecurity

"There's been this steady drumbeat of guidances and policies coming out from the FDA and that's just the nature of cybersecurity and it has to continue to evolve."

-Cybersecurity Program Manager, FDA Office of the Center Director

FDA Defines 'Trustworthy' as

A medical device containing hardware, software, and/or programmable logic that:
- is reasonably secure from cybersecurity intrusion and misuse;
- provides a reasonable level of availability, reliability, and correct operation;
- is reasonably suited to performing its intended functions; and
- adheres to generally accepted security procedures

Trustworthy devices may be more likely to meet the statutory standard for premarket review.

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (draft 2018 p.11)

FDA Cybersecurity Risk Tiers

Tier 1 RISK

"Higher Cybersecurity Risk"

- The device can connect (e.g., wired, wirelessly) to another medical or non-medical product, a network, or Internet; AND
- A cybersecurity incident affecting the device could directly result in patient harm to multiple patients

FDA Premarket Submission Recommendations

- Manufacturers design devices that are trustworthy
- Include documentation demonstrating how the device design
- Include a Risk Management report that includes all 16 topic subcategories

Tier 2 RISK

"Standard Cybersecurity Risk"

- A medical device for which the criteria for a Tier 1 device are not met.

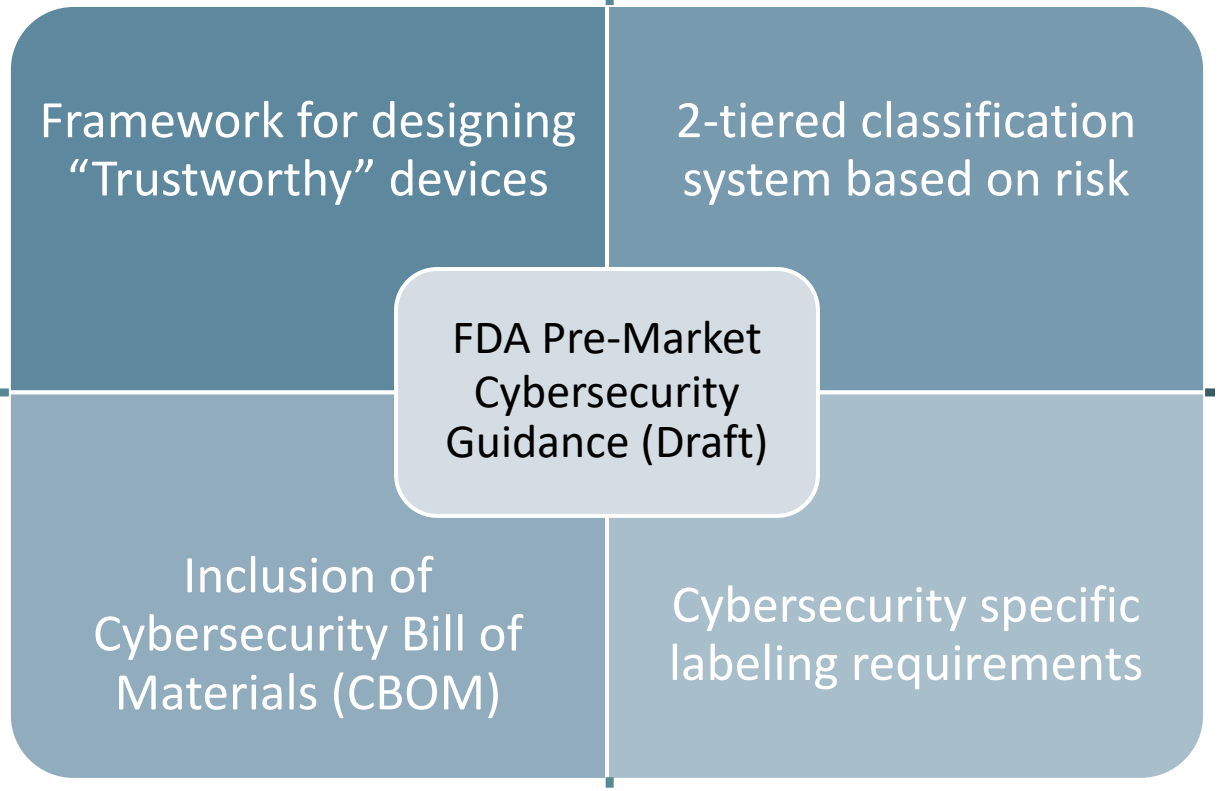
FDA Premarket Submission Recommendations

- Manufacturers design devices that are trustworthy

All text sourced from FDA Content for Premarket Submissions for Management of Cybersecurity in Medical Devices (DRAFT 2018)

Medical Device Cybersecurity

- Recommend following NIST framework
  - **C**onfidentiality
  - **I**ntegrity
  - **A**ccessibility



- **Tier 1**
  - Address all of FDA Guidance design controls
- **Tier 2**
  - Address all design controls or provide risk-based rationale

- CBOM is a subset of the SBOM (Software Bill of Materials)

- Instructions for implementing security measures
- List of interfaces expected to send/receive data
- Accurately inform user of risks and intended use

Cybersecurity & Device Total Product Lifecycle

Goal: Demonstrate cyber risk capabilities throughout the device lifecycle

1

Cyber risk procedures and standards used at every stage of device lifecycle

2

Method to identify controlled and uncontrolled cyber risk (postmarket countermeasure updates and patches)

Do I need FDA clearance or approval?

Let's Execute Your Submission

- OTS
- Hazard Analysis
- SRS/SDS
- Architecture Diagram
- V&V
- Traceability Analysis
- Software Development Environment

Architecture Design Chart

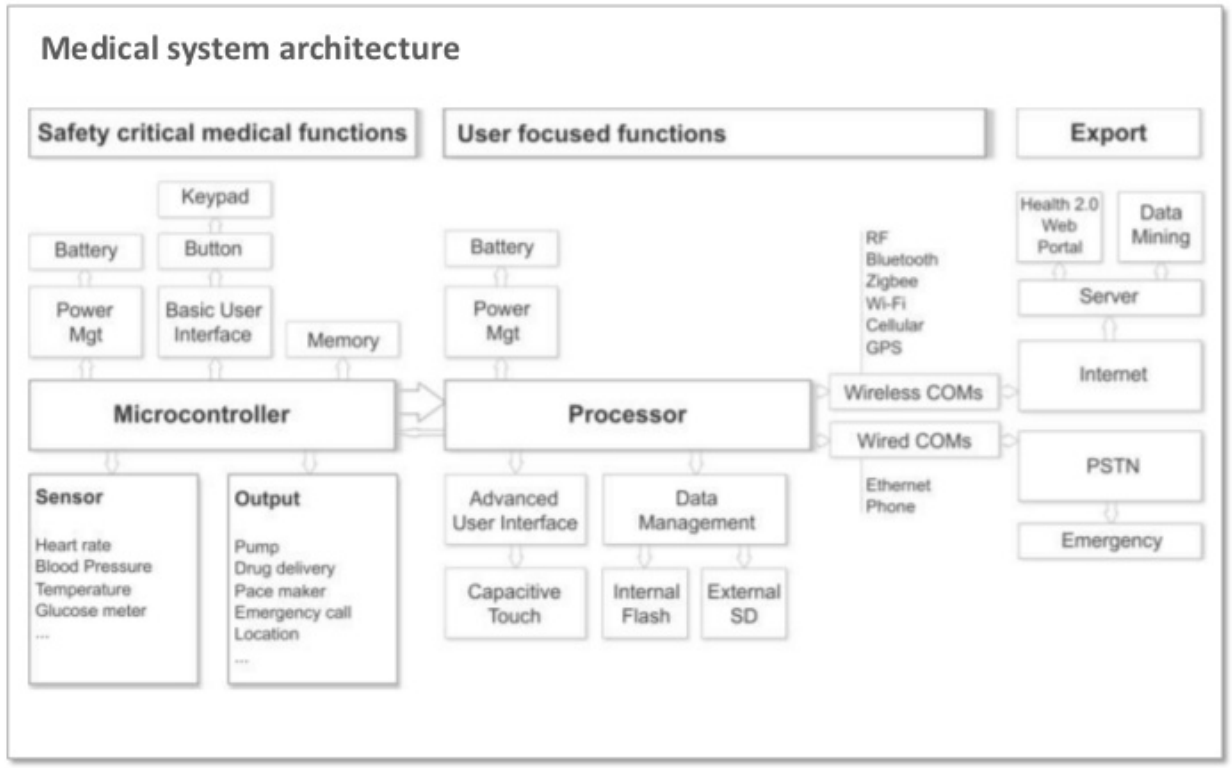
Goal: provide a “legend” for software description

IEC 62304

Demonstrate how device components work together successfully

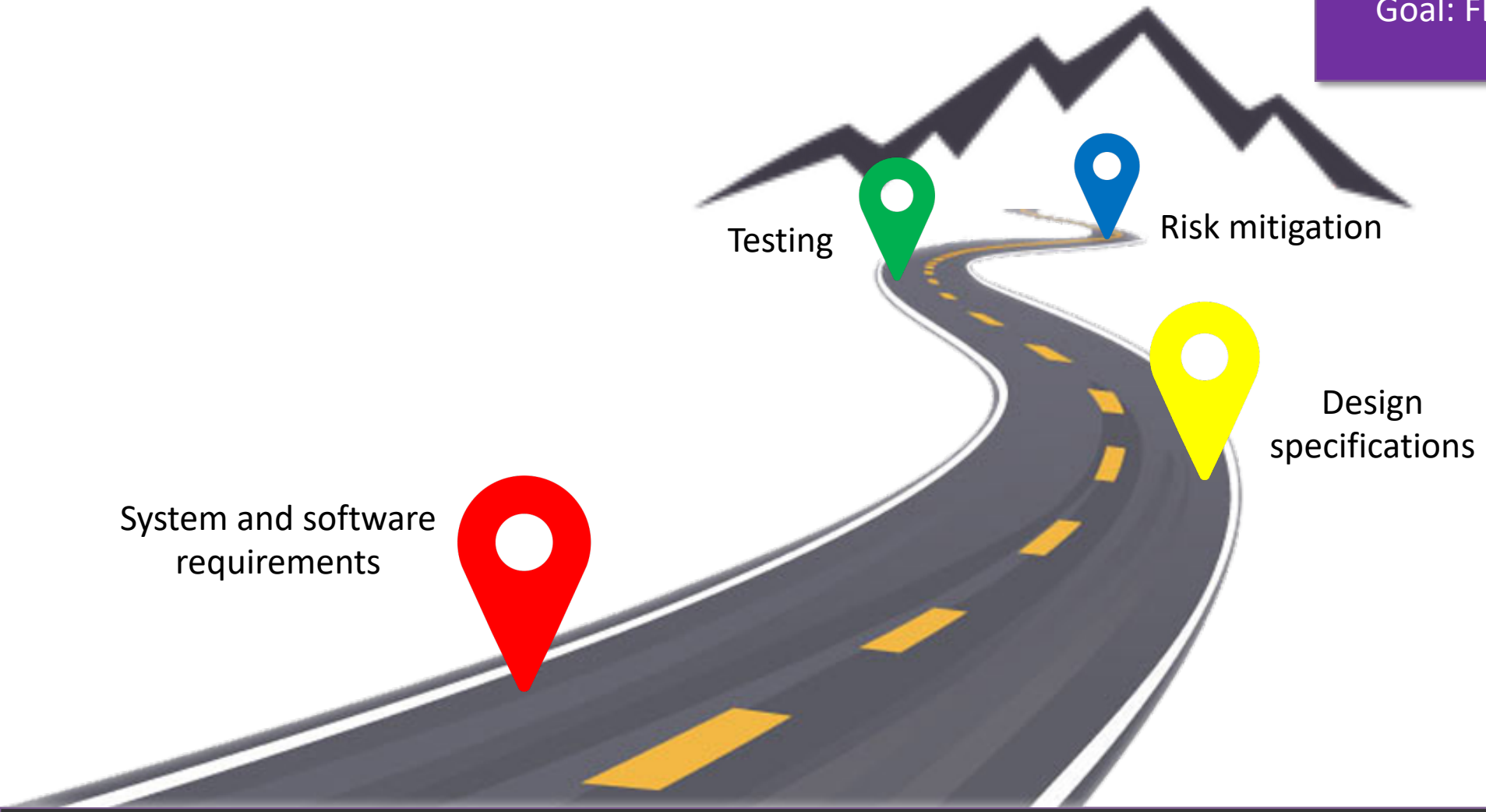
FDA Guidance

High-level visual representation of relationships between major components

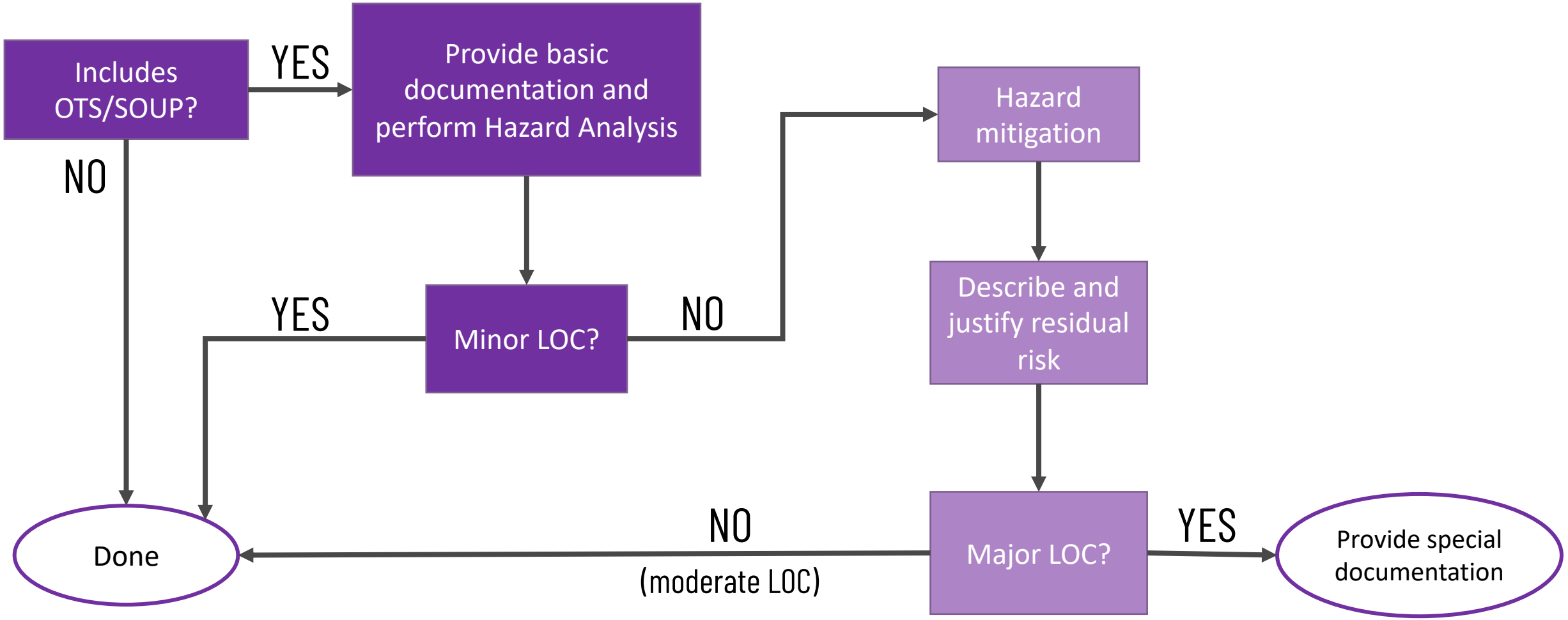


Traceability Analysis

Goal: FDA review roadmap



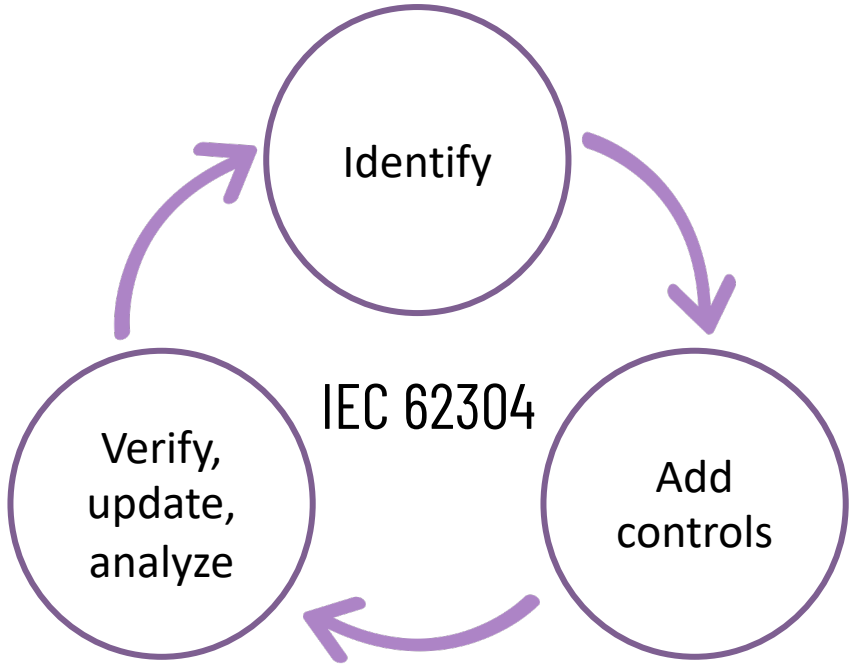
Off-the-Shelf (OTS)/Software of Unknown Providence



Device Hazard Analysis

Goal: Demonstrate that measures control hazards to acceptable level

Required for all levels of risk



FDA

Identification of Hazard	Severity	Cause(s)	Method of control	Mitigating measures taken	Verification of method of control
New entry for each hazard, including any from misuse					

Software Requirement Specification (SRS)

The "What"
of software documentation

IEC 62304

Requirements for:
- Functionality
- Input/output
- Interfaces
- Operator messages
- Security
- Databases
- IT

- "Software development inputs"
- Verify implementation and that there are no contradictions

FDA Guidance

Requirements for:
- Hardware
- Programming language
- Interfaces
- Software

For all Levels of Concern

- Should be testable
- All hazards addressed

Software Design Specification (SDS)

The "How"
of software documentation

IEC 62304

- Not explicitly mentioned
- Divide software into subunits with a design for each unit (Class B, C)

FDA Guidance

- Moderate, Major
- How intended use, safety, and effectiveness are achieved
- Created in a clear and well-defined manner with minimal ad hoc design decisions

One of the most common deficiencies issued by FDA

Verification + Validation

Verification

- Device meets applicable requirements
- Walk-throughs, static and dynamic analyses, code inspection, integration testing, etc.

Validation

- Device does what it's supposed to do, and meets:
  - Intended use
  - User expectations

Verification + Validation

MAJOR LOC

- Document tests failed and changes made as a result
- Proof that changes were effective

MODERARTE LOC

- Traceability analysis

MINOR LOC

- Documentation of device level testing and integration testing
- Pass/fail criteria
- Summary of results

Software Development Environment Description

Goal: Reviewer understands methodology used throughout software lifecycle

1

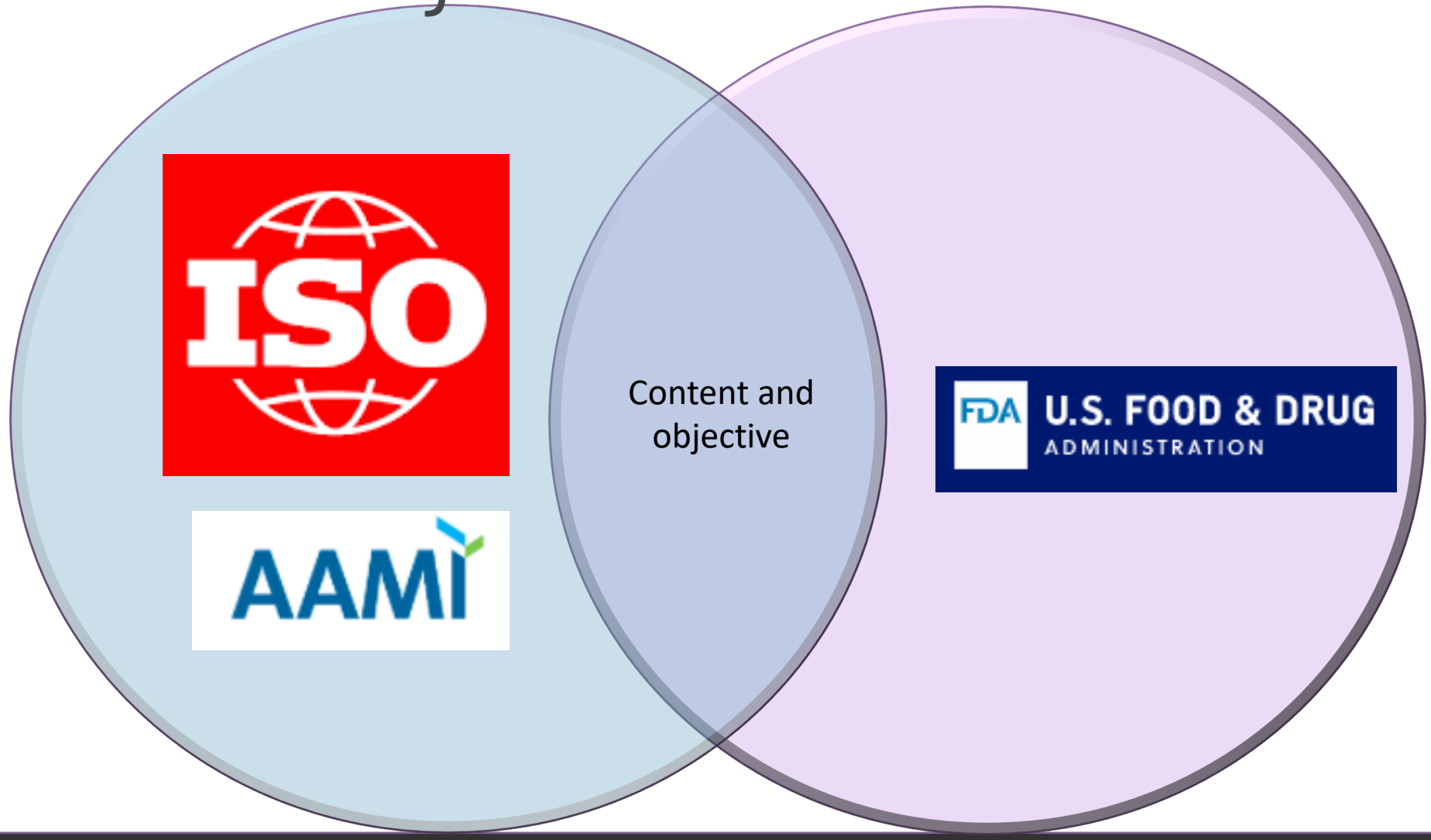
Procedures, standards, and tools used at every stage of product development

2

Plans for configuration management (postmarket updates and changes)

Do I need FDA clearance or approval?

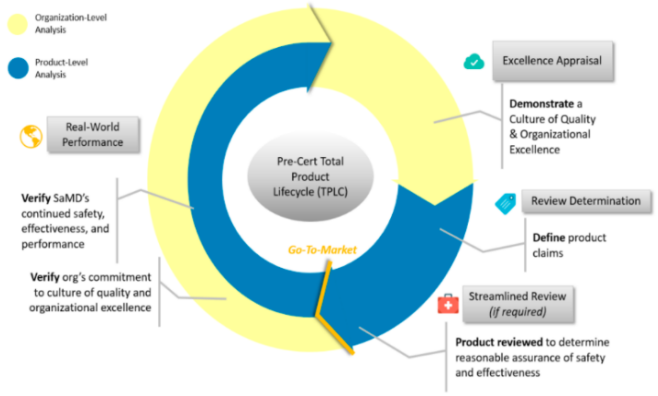
Submission Challenge



Past → Present → Future

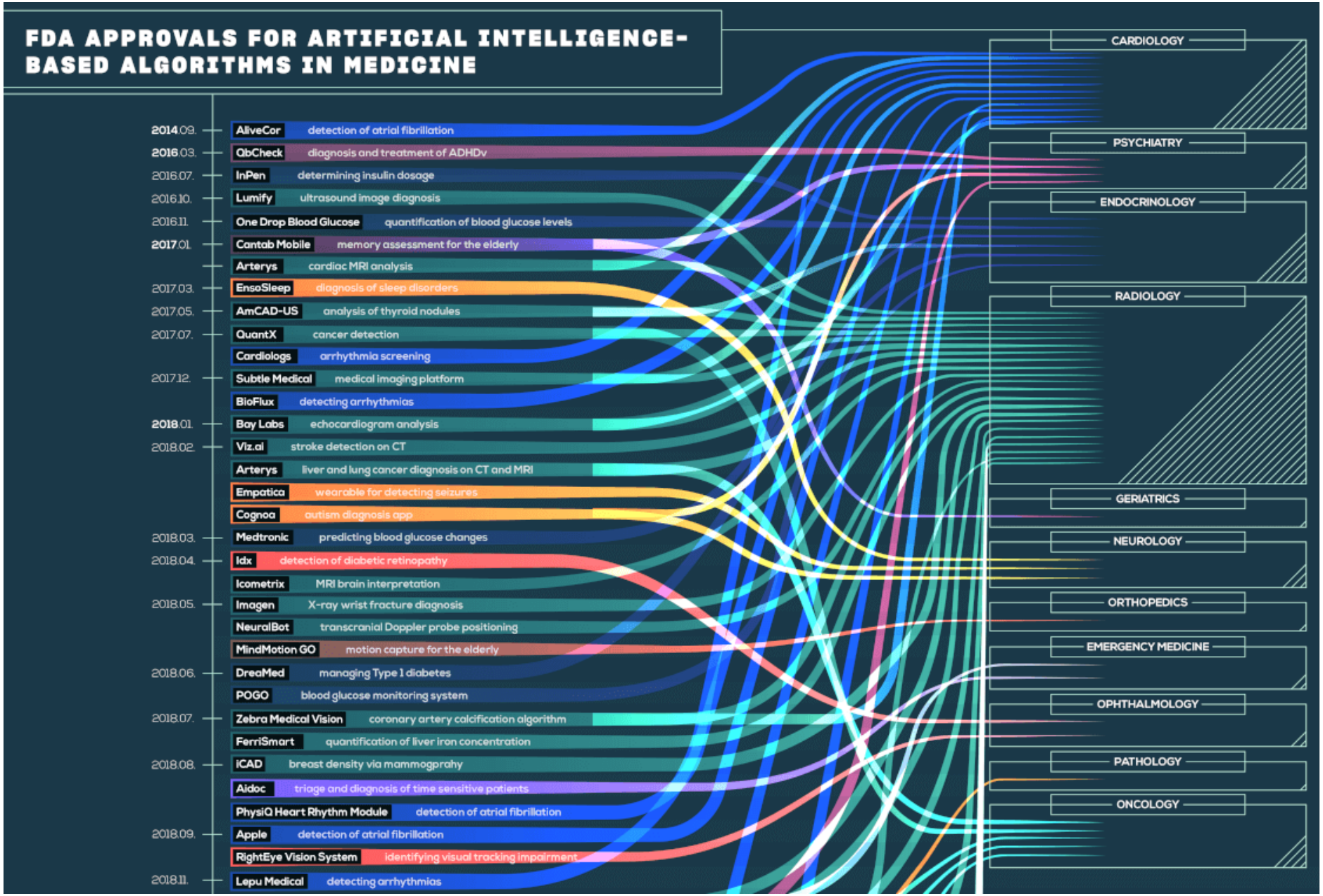
Legislation

Policy Framework



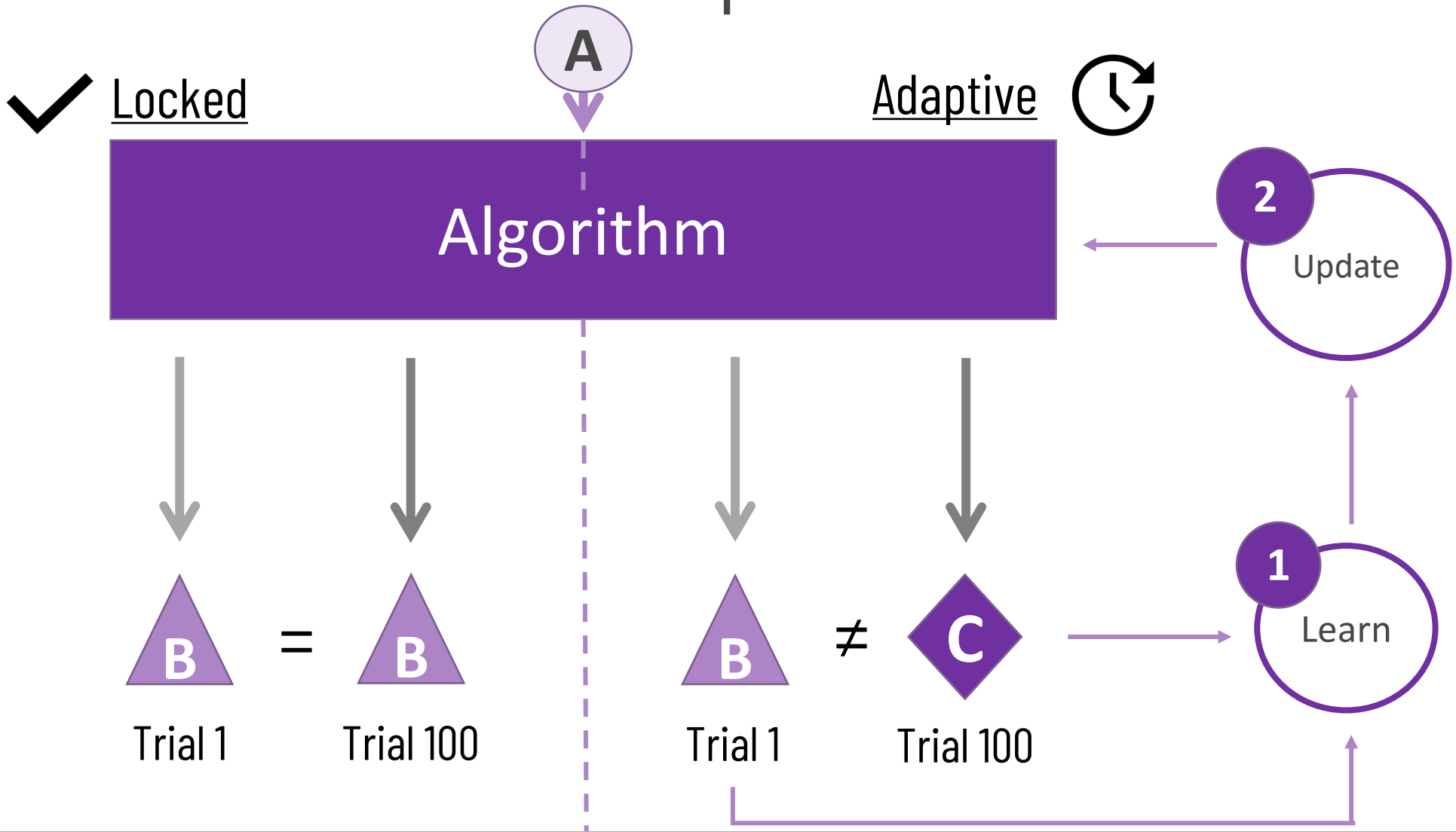
Total Product Lifecycle Approach of the Software Precertification Program

Pilot and Implementation for SaMD



https://cdn.medicalfuturist.com/wp-content/uploads/2019/06/The-Medical-Futurist-FDA-approved-AI-algorithms-in-medicine-2019-09.png

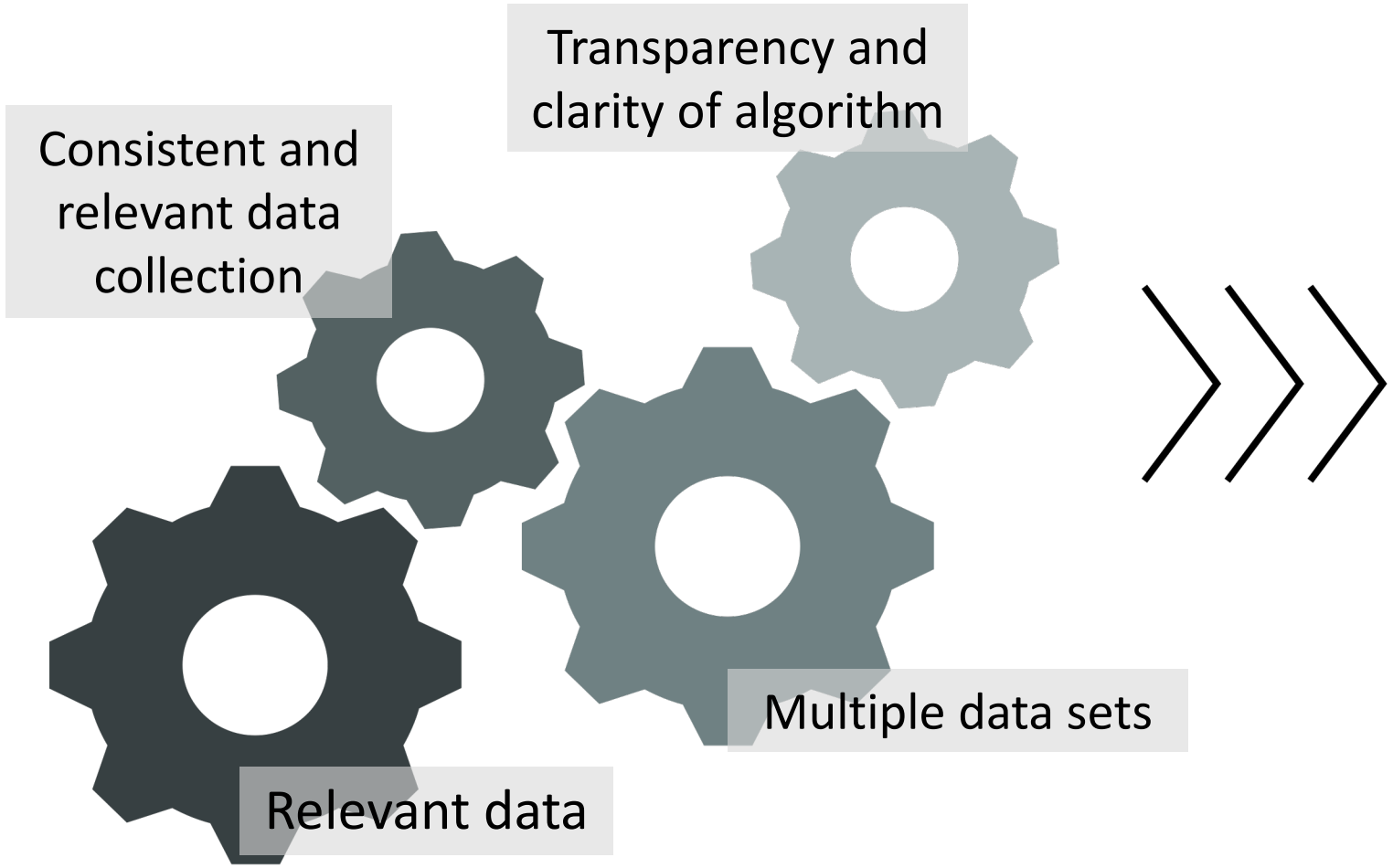
AI Algorithms: Locked vs. Adaptive



Total Product Lifecycle Approach

1. Clear expectations on quality systems and good ML practices
2. Premarket review
3. Risk management plan
4. Increased transparency and real-world monitoring

1. Good Machine Learning Practices (GMLP)



Analytical and Clinical Validation

- Valid association between output, medical condition, and target population
- Generates accurate, reliable, and precise output

2. Premarket Review

The "What"

SaMD Pre-Specifications (SPS):

Anticipated modifications to performance, inputs, or intended use once the algorithm is in use

Draw "region of potential changes" around initial specifications and labeling

The "How"

Algorithm Change Protocol (ACP):

Step-by-step delineation of data and procedures to ensure changes in the SPS meet their goal safely

Protocols for data management, re-training, performance evaluation, and updating procedures

3 Types of Modifications Relating to…

Performance

- Analytical and clinical
- Re-training with new data sets
- Ex: increase sensitivity

Inputs

- Expanding compatibility with other sources of same input type
- Adding input data types

Intended Use

- Change in significance of info
- Change in healthcare situation
- Change in intended disease/condition

4. Increased Transparency

- Postmarket data collecting to demonstrate continued safety and effectiveness
- Having mechanisms and procedures in place to notify how and what is updated
- Update specifications or compatibility of any impacted supporting devices, accessories, etc.
- Accurate label changes that fully describe the modification for changes to SPS and ACP
- Updates to FDA, device companies, collaborators, and public (clinicians, patients)

Take-Aways

Risk, intended use, and intended user determine regulatory oversight

Properly classifying your technology leads to more organized regulatory submission

Integrate cybersecurity considerations early in your design process

Explore all potential pathways for your technology

Complying with standards AND FDA Guidance requires identifying the gaps

Regulatory considerations should be made throughout the product lifecycle

Nikki Batista

nbatista@mcra.com

Associate Director,
Cardiovascular Regulatory Affairs

Former FDA Assistant Director in the Division of Cardiac Electrophysiology, Diagnostics, & Monitoring Devices

Highlights

- Extensive knowledge of digital health medical device regulations and policies
- Additional prior roles at FDA include Senior Lead Reviewer, Peripheral Intervention Devices Team and Lead Reviewer, Interventional Cardiology Devices Branch

Jason Tugman

jtugman@mcra.com

Associate Director,
Cybersecurity Risk Management & Strategy

Brings 15+ years of cybersecurity experience to MCRA's Digital Health franchise

Highlights

- Extensive experience within multiple frameworks (NIST, ISO, etc.), expertise in FDA Premarket & Postmarket Medical Device Joint Security Plan (JSP)
- An active industry speaker and leader of talks regarding FDA cybersecurity in medical devices

Thank you.