CONTRACTS

FDA 2023 Updates

Omnibus Bill

Cybersecurity Insurance

Service Contracts

Gaps or Opportunities

Possible Next Steps

CONTRACTS

2023 FDA Updates

- **Scope of the Guidance**: The updated guidance applies broadly to **all** devices with cybersecurity considerations. This includes devices that have a software function, contain software or **programmable logic**, and are **network-enabled**. It also applies to devices that do not require a premarket submission, such as 510(k)-exempt devices. https://www.fda.gov/media/173516/download

2023 FDA Updates

- **Secure Product Development Framework (SPDF)**: Manufacturers are recommended to implement an SPDF to address cybersecurity risks at each stage of device development. This framework should include a security risk management plan with traceability documentation for threat modeling, cybersecurity risk assessments, and a software bill of materials. https://csrc.nist.gov/Projects/ssdf

- **Device Labeling**: The FDA advises that device labeling should include a clear description of the medical device's cyber risks in a manner understandable to the average user. https://www.fda.gov/medical-devices/overview-device-regulation/device-labeling

Omnibus Bill 2023

Signed

December 29, 2022

Manufacturers

- Must submit a plan to monitor, identify, and address, post-market cybersecurity vulnerabilities and exploits.
- Must submit a plan for coordinated vulnerability disclosure and related procedures
- Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure.

Manufacturers

- Must submit a plan to monitor, identify, and address, post-market cybersecurity vulnerabilities and exploits.
- Must submit a plan for coordinated vulnerability disclosure and related procedures
- Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure.

Manufacturers

- Make available post market updates and patches to the device and related systems to address:
  A. On a reasonably justified regular cycle, known unacceptable vulnerabilities; and
  B. As soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks

- Provide a software bill of materials, including commercial, open-source, and off-the-shelf software components

Cyber Vulnerabilities Per Year

from 2023 to 2025:

📊 Annual CVE Counts

Year	Total CVEs Published	Notable Insights
2023	28,818	Marked a record high at the time.
2024	40,009	Represented a 38% increase from 2023.
2025 (as of April 14)	14,128	On track to potentially exceed 2024's total.

Moving Forward

Cyber Insurance

Prediction #1: Third party misconfigurations will lead to more cyber insurance claims.

- Example; Cloud misconfigurations will continue to grow as a threat vector due to increased adoption rates and poor security policies

Cyber Insurance

Prediction #2: Carriers will consider organizations with less risky behavior

- Organizations will need to show the cyber insurance underwriter that they have effective cybersecurity policies and countermeasures in place that make them less risky.

Cyber Insurance

Prediction #3: Vulnerability prioritization capabilities will become crucially important.

- Most businesses have a patching strategy in place. An underwriter will look kindly upon organizations that can demonstrate that they have the right security solution in place for centralized, proactive, and defragmented monitoring, tracking, analysis, identification, and detection of vulnerable areas.

- **Prediction #4: Businesses will be required to have a "second set of eyes" to contain policy costs.**
  - When renewing a policy, carriers need assurance that an organizations' security posture has evolved with the threat landscape to minimize cyber risk.

Cyber Insurance

Prediction #3: Vulnerability prioritization capabilities will become crucially important.

- Most businesses have a patching strategy in place. An underwriter will look kindly upon organizations that can demonstrate that they have the right security solution in place for centralized, proactive, and defragmented monitoring, tracking, analysis, identification, and detection of vulnerable areas.

Cyber Insurance

- **Result: Increased Demand and Premiums for Cybersecurity Insurance**

As the threat landscape for medical devices continues to evolve and the regulatory environment becomes more stringent, hospitals are likely to face increased risks associated with cyberattacks.

- **Result: More Stringent Underwriting Criteria**

Insurers may develop more rigorous underwriting criteria for medical device cybersecurity policies. This could include assessments of a hospital's cybersecurity practices, the types of medical devices used, and their vulnerability to cyber threats.

Cyber Insurance

- **<u>Result:</u> Integration of Cybersecurity Standards in Insurance Policies**

Future cybersecurity insurance policies for medical devices might require compliance with specific cybersecurity standards or frameworks. This integration would ensure that hospitals are adhering to best practices in securing their devices.

Service Contracts with the Cybersecurity Components

- Difference scope
- Difference in requirements
- Difference in stakeholder
- expectations/accountability
- Difference in resource competency requirements

Service Contracts In the Past

- Service Calls Onsite or Remote
- Scheduled Preventative Maintenance
- Disposables/Supply Consumption
- Depot/Onsite Repairs
- Device Exchanges

Service Contracts Moving Forward Cybersecurity Components

Vulnerability Management

Incident Response Requirements

Indemnity Insurance

Auditable Vendor Documentation

Service Contracts Moving Forward

Vulnerability Management

- Notifications
- Patching
- What devices are included (Additional devices like firewalls)
- OS/Application/Third Party

Service Contracts

Moving Forward

Incident Response Requirements

- Defined Response Timeframes
- Designated lead Incident Resource
- Documentation Deliverables (initial impact analysis, IR plan)
- (Additional devices)
- OS/Application/Third Party

Service Contracts

Moving Forward

Indemnity Insurance

- Who pick up the tab when a device is infiltrated from a remote connection or a local attack.

Service Contracts Moving Forward

Auditable Vendor System

and

Remote Networking

Compliance Documentation

Gaps Or Opportunities

New Contract Requirements/Contract Addendums

Asset Management

Database Asset/Incident Management

Cybersecurity Medical Device Contract Evaluator/Auditor

Resource Cybersecurity Knowledge Base

New Contract Requirements/Contract Addendums

Does your health system have medical device cybersecurity requirements to propose/negotiate in contracts?

Asset Management

Are there enough **searchable** fields to include cybersecurity required fields for (SBOM details, encryption, wired and wireless details…)

Database Asset/Incident Management

Is there unified incident response workflow attached to the medical device/system.

Are vendors providing documentation identifying when vulnerability patches are implemented and Are Cybersecurity Incidents and vulnerability patches a searchable field in the asset management database

Cybersecurity Medical Device Contract Evaluator/Auditor

Who reviews the cybersecurity components for the medical devices and audits vendor for compliance.

Resource Knowledge Base

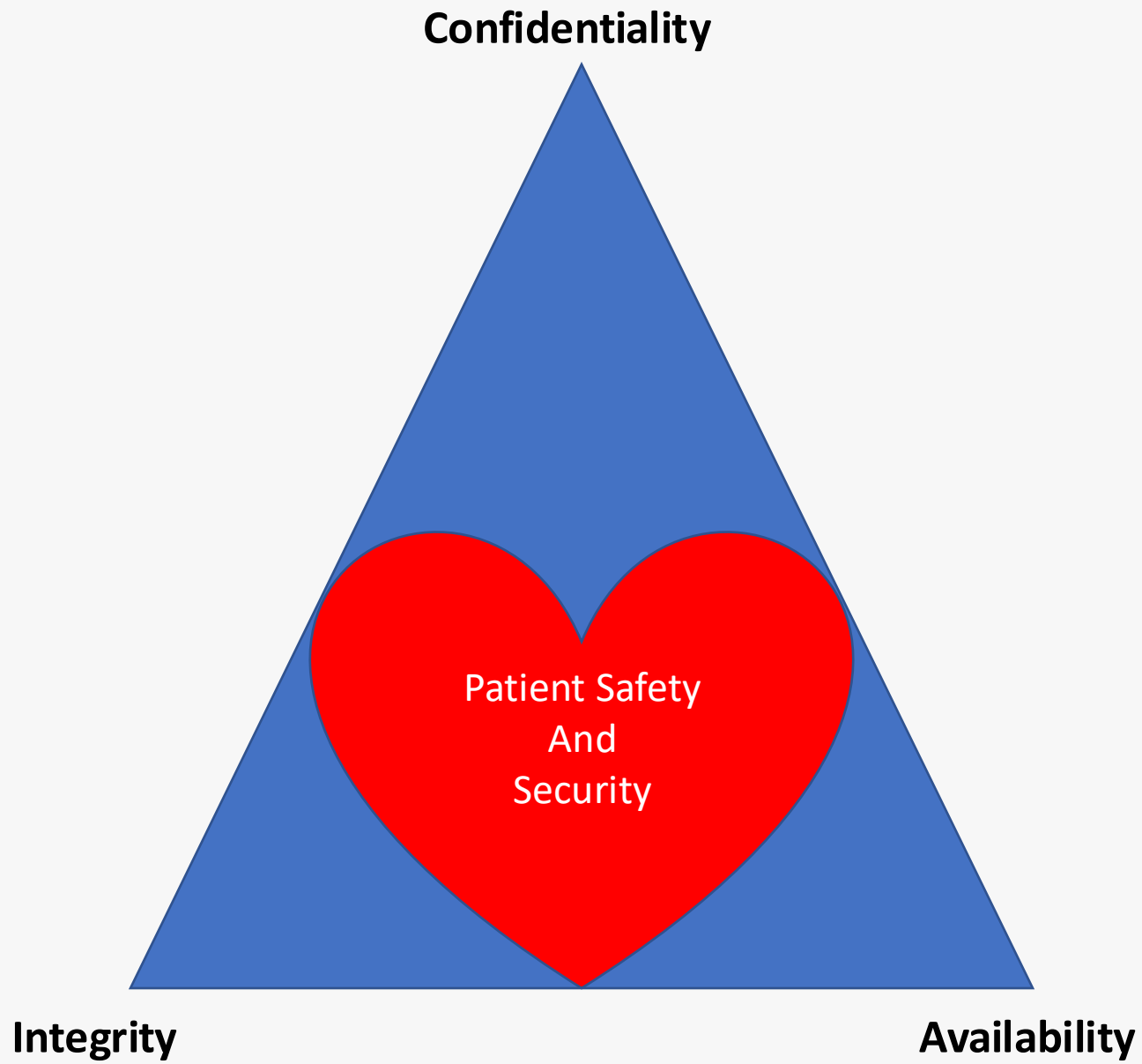
Cybersecurity

Medical Device Industry requirements and standards

Medical Device configurations and Integrations

Legal/ Contracts with Cybersecurity Requirements

Healthcare Cybersecurity Mindset



Possible Next Steps

Identify your medical device cybersecurity resources (Biomed, IS, Legal)

Develop a list of cybersecurity deliverables that the health system would want to have included new purchases and service contracts.

- Identify and prioritize the deliverable that are **must** haves and which ones are **nice** to have.

Possible Next Steps

Review all new purchases and service contracts coming up for renewal for incorporating any cybersecurity deliverables.

Submit the request of the cybersecurity requirements to be added to the purchase agreements/service contracts.

Negotiate based on industry requirements and standards

QUESTIONS?