Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

Clearwater

Healthcare – Secure, Compliant, Resilient

New Cybersecurity Requirements for Medical Devices: Insights & Actions for Manufacturers

June 7th, 2023

Agenda

- Understanding the FDA Regulatory Landscape:
- 524B Regulatory Requirements
- Compliance Strategy Approaches & Recommendations
- Q&A

Clearwater Team – Consulting Services

hy Homstad, CISSP, CISA, CIPP/US

or, Security and Compliance

services leader with 16+ years of experience managing compliance, audit, cyber-security, and data privacy risks for Fortune 100 and Fortune 500 companies.
across multiple industries, including manufacturing, government, healthcare, engineering, banking, retail, financial services, and higher education.
Clearwater providing business leadership, strategic initiatives planning, new services development, managed multiple delivery teams, and provided
ng partnerships to dozens of clients.
r expert level understanding across many compliance frameworks, including but not limited to; NIST-800-53, HIPAA, GDPR, ISO 27001, NIST-171, NIST-800-
IT, SOC 2, Sarbanes-Oxley
r expert across security and technology risk domains; including access/identity management, operations security, cryptography controls, governance,
security, third party risk management, incident management, business continuity, data retention, logging/monitoring controls, amongst others.
ort and advocacy through multiple organizations:
rmation Systems Audit and Control Association (ISACA; 2007-Present)
rnational Information System Security Certification Consortium (ISC^2; 2015-Present)
rnational Association of Privacy Professionals (IAPP; 2016-Present)

linkedin.com/in/timothyhomstad/

About Your Presenter

Jacob Carroll, MBA, CISSP, CISA, CIPP, CDPSE

Vice President, Consulting Services

- 17+ years of technical consulting experience, with deep understanding of risk management across multiple industries and market segments including healthcare, manufacturing, finance, retail, education, and non-profits
- Big4 consulting background with numerous industry recognized certifications validating expertise across multiple skill disciplines including cybersecurity, IT audit, and data privacy.
- 9+ years with Clearwater providing business operations leadership, strategic initiatives planning, new services development, and overseen multiple delivery teams.
- 8+ years of Medical Device Manufacturing & Healthcare Sector consulting experience; holding roles to enhance data privacy compliance (HIPAA, CCPA, GDPR) and implementation of internal controls (ISO, NIST, CSA, etc.)
- Industry support and advocacy through multiple organizations:
- Information Systems Audit and Control Association (ISACA; 2007-Present)
  - Board Member – Cybersecurity Nexus Liaison (2015-2017)
- International Information System Security Certification Consortium (ISC^2; 2014-Present)
- International Association of Privacy Professionals (IAPP; 2016-Present)

https://www.linkedin.com/in/jacobcarroll/

Omnibus Bill History & FD&C Act

- Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law on December 29th, 2022.
  - Section 3305 “Ensuring Cybersecurity of Medical Devices” amended FD&C Act with section 524B
  - Section 524B went into effect March 29, 2023
- The Food, Drug, and Cosmetic Act (FD&C Act) is the primary law that governs the safety and effectiveness of medical devices in the United States.
  - The FD&C Act requires manufacturers to submit premarket applications (PMAs) for certain high-risk devices.
  - The FDA also has postmarket authority to require manufacturers to take corrective and preventive action (CAPA) if a device is found to be unsafe or ineffective.
  - Going forward, FDA will issue Refuse to Accept if 524B objectives not met

Medical Device Industry Impact

- Manufacturers will need to develop and implement comprehensive cybersecurity programs to ensure the safety and security of their devices.
- Applies to all medical devices which:
  1. includes software validated, installed, or authorized by the sponsor as a device or in a device;
  2. has the ability to connect to the internet; and
  3. contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.
- FDA to issue a Refuse to Accept (RTA) for submissions without sufficient documentation for items defined in 524B
  - FDA likely won't RTA solely on 524B prior to October 1st, 2023.

How to Determine Your Organization's Scope Applicability

- New submissions which were filed prior to March 29th, 2023 are not be impacted by the new requirements
  - Submissions filed prior to October 1st, 2023 *should* comply with the new requirements, but FDA likely to not reject.
  - Submissions filed after October 1st, 2023 ***must*** comply with new requirements
- The new cybersecurity requirements apply to all medical devices that are "connected to or interoperable with a network."
  - Example: Mobile Medical Apps, Biomedical Devices, Physiological Monitors, Programmers, etc.
  - This includes devices that are connected to the internet, as well as devices that are connected to internal networks.
    - Includes: Wireless/wired, Bluetooth/LE, etc.
- Manufacturers of these devices will need to develop and implement a cybersecurity program that is appropriate for the risks associated with their products.

524B Regulatory Requirements

- Manufacturers must develop and implement a risk management plan which monitors, identifies and assesses the cybersecurity risks associated with their devices.
- Manufacturer’s cybersecurity program will need to include measures to protect devices from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Manufactures must provide a software bill of materials (SBOM)
- Manufacturers must update their cybersecurity programs as needed to address new risks.

Medical Device Cybersecurity Plan Development

- The first step in developing a medical device cybersecurity plan is to identify and assess the cybersecurity risks associated with the device.
- This includes identifying potential threats and vulnerabilities, as well as the potential impact of a cybersecurity incident.
- Once the risks have been identified and assessed, the manufacturer can develop and implement measures to mitigate the risks.
- Some of the measures that can be taken to mitigate cybersecurity risks include:
  - Implementing security controls, such as firewalls and intrusion detection systems
  - Educating employees about cybersecurity risks
  - Conducting security audits and penetration tests
  - Maintaining security documentation

Postmarket Vulnerability Management & Disclosures

- Once a medical device is on the market, it is important to monitor for vulnerabilities and to disclose them to the FDA in a timely manner.
- The FDA requires manufacturers to report cybersecurity vulnerabilities to the agency if the vulnerability could impact patient safety or clinical performance of the device
- This allows the FDA to take steps to protect patients and to inform other manufacturers of the vulnerability.

In-Field Medical Device Impact & Approach Considerations

- When developing a cybersecurity plan, it is important to consider the impact of cybersecurity incidents on in-field devices.
- This includes the potential for devices to be compromised, the potential for data to be lost or stolen, and the potential for devices to be used to harm patients.
- The manufacturer should develop an approach that addresses the potential impact of cybersecurity incidents on in-field devices. This approach should include measures to:
  - Detect and respond to cybersecurity incidents
  - Protect patient data
  - Restore devices to operation after a cybersecurity incident

Development of Repeatable Program Operating Procedures

- The manufacturer should develop and implement repeatable program operating procedures (POPs) for their cybersecurity program.
- These POPs should document the steps that the manufacturer will take to implement and maintain their cybersecurity program.
- The POPs should be clear, concise, and easy to follow.

Validating Effectiveness of Medical Device Patch & Vulnerability Management Practices

- The manufacturer should validate the effectiveness of their medical device patch and vulnerability management practices.
- This can be done by conducting regular audits and penetration tests.
- The audits and penetration tests should identify any weaknesses in the manufacturer's patch and vulnerability management practices.

Determining Unacceptable Vulnerabilities and Uncontrolled Risks

- The manufacturer should determine which vulnerabilities are unacceptable and which risks are uncontrolled.
- Unacceptable vulnerabilities are those that could pose a significant risk to patient safety or the security of the device.
- Uncontrolled risks are those that have not been mitigated or that are not being monitored.

Exemptions and Future Additions to the Med Device Landscape

- There are several exemptions to the new cybersecurity requirements. These exemptions include:
  - Devices that are not connected to a network
  - Devices that are not used in patient care
  - Devices that are used in research.
- The FDA is expected to add additional requirements to the new cybersecurity framework in the future.

Key take aways for OEMs: Cybersecurity Plan Development

Monitor, identify, and address postmarket cybersecurity vulnerabilities and exploits

- Monitoring System: Regular vulnerability scans and threat intelligence monitoring.
- Vulnerability Assessment: Use the CVSS for severity scoring, considering access, user interaction, and system impact.
- Disclosure Process: Clear instructions for submitting vulnerability reports and communicating with stakeholders.
- Addressing Vulnerabilities: Prioritize based on severity and patient safety. Develop a mitigation plan.

Key take aways for OEMs: Cybersecurity Plan Development

- Risk Management: Implement regular security updates and vulnerability scanning.
  - Monitor, identify, and address postmarket cybersecurity vulnerabilities and exploits
- FDA Reporting: Describe the vulnerability, its impact, and actions taken.
- Training: Focus on the importance of cybersecurity, secure coding practices, and cybersecurity awareness.

Key take aways for OEMs: Cybersecurity Plan Development

- Risk Management Team: Multidisciplinary team from various departments like engineering, quality, legal, regulatory, security, and IT.
- Risk Management Plan: Outline steps for risk assessment, mitigation, and ongoing monitoring across device lifecycle.
- Cybersecurity Controls: Regular updates, ITGCs, change management, access controls, physical security, data encryption, and end-user training.
- Monitoring and Evaluation: Regular vulnerability assessments and testing of incident response protocols.
- Post-market Surveillance Plan: Monitoring and analyzing cybersecurity risks after product release, and procedures for postmarket updates.
- Post-market Updates: Thoroughly tested and validated updates and patches to mitigate identified cybersecurity risks.

Key take aways for OEMs: Cybersecurity Plan Development

- Identify, document and track all software components used within your products, including:
  - Off the shelf software
  - Customer or commercial software
  - Open-source libraries

Software Bill of Materials

Q&A

Steve Cagle
Steve Akers
Justin Sun

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare – Secure, Compliant, Resilient

Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394