

**SAFEGUARDING
HEALTH
INFORMATION:
BUILDING
ASSURANCE
THROUGH HIPAA
SECURITY 2024**

WASHINGTON, DC



OCTOBER 23-24 2024
HOSTED BY NIST & HHS



**Safeguarding Health Information:
Building Assurance Through HIPAA Security Conference**

Deputy Secretary Andrea Palm



2024 Cyber Threat Landscape: A Strategic and Tactical Overview

Global Overview of Cyber Threats

1

Increasing Sophistication

Global attacks have become more targeted, with a significant rise in zero-day vulnerability exploitation. The Colonial Pipeline attack in 2021 by the DarkSide ransomware group disrupted 45% of the U.S. East Coast's fuel supply, demonstrating the far-reaching impact of sophisticated cyber attacks.

2

Rising Geopolitical Tensions

State-sponsored cyberattacks are increasingly targeting critical infrastructure and supply chains. The NotPetya attack in 2017, initially targeting Ukrainian infrastructure, spread globally and caused over \$10 billion in damages, highlighting the potential for cyber warfare to have widespread economic consequences.

3

Evolving Attack Vectors

The 2023 MOVEit data breach, perpetrated by the Clop ransomware group, exploited a vulnerability in a widely-used file transfer tool, affecting hundreds of organizations. This incident underscores the growing trend of attackers targeting widely-used software to maximize impact.

Nation-State Threat Actors



Global Reach

Nation-state threat actors operate globally, launching cyberattacks from countries like Russia, China, North Korea, and Iran.



Sophisticated Attacks

These groups employ advanced techniques and tools, posing significant challenges to cybersecurity defenses.



Targets

Critical infrastructure, intellectual property, and sensitive government data are prime targets for nation-state actors.



International Cooperation

Combating these threats requires international cooperation and sharing of intelligence to prevent and mitigate attacks.

These groups, often backed by government resources, engage in long-term campaigns targeting critical infrastructure, intellectual property, and sensitive government data. The NotPetya attack, attributed to Russia, demonstrated the devastating potential of nation-state cyberweapons, causing billions in damages globally.

China's APT41 group, known for its Operation Cloud Hopper campaign, exemplifies the focus on intellectual property theft and economic espionage. As geopolitical tensions rise, the frequency and sophistication of nation-state cyber operations are expected to increase, necessitating robust, multi-layered defense strategies and international cooperation to combat these threats.

Major Threat Actors Overview



APT28 (Fancy Bear)

This Russian group focuses on espionage, targeting military, government, and election systems. Their involvement in the 2016 U.S. election interference, including hacking the Democratic National Committee (DNC), demonstrates their capacity for large-scale, politically motivated cyber operations.



Lazarus Group

This North Korean actor targets financial institutions and cryptocurrency exchanges. Their audacious 2016 Bangladesh Bank heist attempt, where they tried to steal nearly \$1 billion using the SWIFT banking system, showcases their financial motivation and sophistication.



APT41 (Double Dragon)

This Chinese group blends espionage with cybercrime, targeting sectors like healthcare and telecommunications. Their ongoing Operation ShadowPad, which uses backdoor malware in trusted software updates to steal intellectual property globally, highlights their persistent and evolving threat.

Advanced Persistent Threat (APT) Groups



APT29 (Cozy Bear)

This Russia-backed group specializes in espionage and was responsible for the SolarWinds attack in 2020. By compromising SolarWinds' software update system, they gained unprecedented access to U.S. government agencies and corporations, demonstrating the severe impact of supply chain attacks.



Hafnium (China)

Hafnium gained notoriety for exploiting Microsoft Exchange vulnerabilities in 2021. Their exploitation of the ProxyLogon vulnerability compromised over 250,000 servers globally, showcasing their ability to rapidly exploit newly discovered vulnerabilities at scale.



APT41 (Double Dragon)

This Chinese group continues to blur the lines between state-sponsored espionage and cybercrime. Their diverse targeting, from healthcare to high-tech sectors, and their use of sophisticated tools like ShadowPad, make them a persistent and adaptable threat.



Lazarus Group

North Korea's Lazarus Group remains a significant threat, particularly to financial institutions and cryptocurrency exchanges. Their operations often aim to generate revenue for the regime, making them a unique hybrid of state-sponsored actor and cybercriminal group.

Ransomware Groups



LockBit 3.0

As a leading Ransomware-as-a-Service (RaaS) platform, LockBit 3.0 employs advanced extortion techniques. Their 2021 attack on Accenture, demanding \$50 million in ransom, showcases their audacity in targeting high-profile corporations. LockBit's constantly evolving tactics and its affiliate model make it a persistent and adaptable threat.



BlackCat (ALPHV)

BlackCat specializes in targeting high-value enterprises with advanced encryption methods. Their attack on energy company Schneider Electric in 2022 caused significant operational disruptions, highlighting the potential for ransomware to impact critical infrastructure. BlackCat's use of the Rust programming language demonstrates the group's technical sophistication.



Clon Ransomware

Clon has gained notoriety for exploiting third-party vulnerabilities, as seen in the widespread 2023 MOVEit exploit. This attack affected numerous organizations globally, demonstrating Clon's ability to leverage supply chain weaknesses for maximum impact. Their tactic of exploiting widely-used software makes them a significant threat to organizations of all sizes.

Cybercrime Syndicates



FIN7 (Carbanak)

FIN7 specializes in point-of-sale (POS) attacks and ATM malware. Their 2017 breach of Chipotle's POS systems, stealing payment card data from millions of customers, exemplifies their focus on financial gain through large-scale data theft. FIN7's sophisticated malware and social engineering tactics make them a formidable threat to retail and hospitality sectors.



Evil Corp (Dridex)

Known for banking Trojans and ransomware deployment, Evil Corp has been targeting European banks with increasing sophistication. Their use of the Dridex malware to attack financial institutions in 2019 showcased their ability to evolve their tactics and target high-value victims. Evil Corp's operations blur the line between cybercrime and state-sponsored activities.



Conti Group Legacy

Although the original Conti group disbanded, its splinter groups continue to operate under different names. The 2022 attack on the Costa Rican government, which disrupted national services for weeks, demonstrates the ongoing threat posed by these offshoots. The Conti legacy groups' ability to quickly rebrand and adapt makes them a persistent threat in the ransomware landscape.

AI-Driven Attacks

AI-generated Phishing

Machine learning is revolutionizing phishing campaigns by creating highly personalized and convincing messages. The 2019 deepfake CEO fraud case, where attackers used AI-generated audio to impersonate a CEO and steal \$243,000 from a UK energy company, illustrates the potential for AI to enhance social engineering attacks. As AI technology advances, we can expect these attacks to become more sophisticated and harder to detect.

AI in Vulnerability Scanning

AI tools are automating the discovery of zero-day vulnerabilities at an unprecedented scale. Recent cases of AI-driven reconnaissance on industrial control systems demonstrate how these tools can rapidly scan critical infrastructure networks to identify weaknesses. This capability could significantly reduce the time between vulnerability discovery and exploitation, putting pressure on organizations to improve their patching processes.

AI-powered Malware

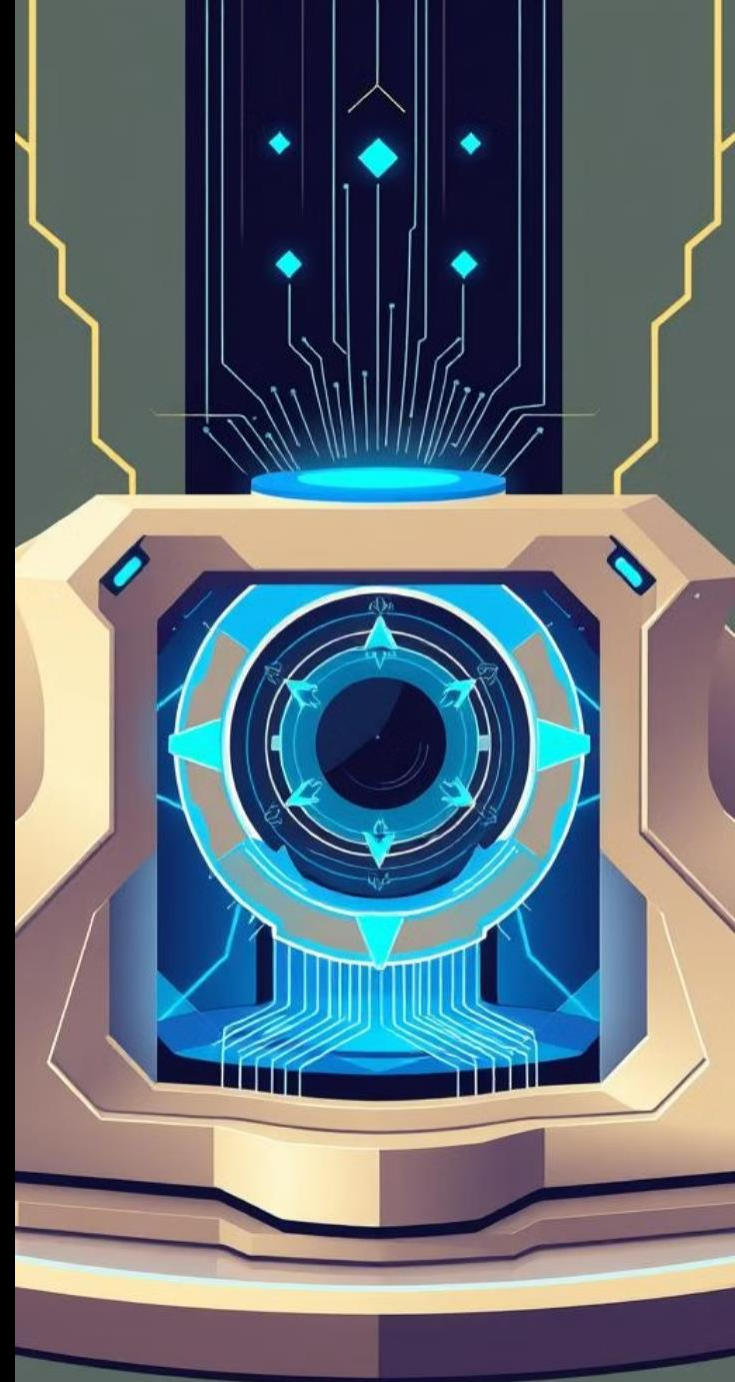
Self-learning malware that adjusts its behavior to avoid detection is emerging as a serious threat. While still largely theoretical, AI-enabled malware targeting critical infrastructure for persistent attacks could potentially learn from defense mechanisms and adapt in real-time. This could lead to malware that is extremely difficult to detect and eradicate, posing significant challenges for traditional security measures.



Quantum Computing

| Threat | Impact | Mitigation |
|---------------------------------|---|---|
| Breaking RSA and ECC encryption | Compromised data security, privacy violations | Development of quantum-resistant algorithms |
| Geopolitical quantum race | Potential cyber supremacy for leading nations | International cooperation and regulations |
| Legacy systems vulnerability | Long-term data exposure | Early adoption of post-quantum cryptography |

Quantum computing poses a significant threat to current encryption standards. Algorithms like Shor's could potentially break RSA and ECC encryption in minutes, rendering much of our current secure communication vulnerable. Simulations have already demonstrated this theoretical capability, underlining the urgency of developing quantum-resistant cryptography. The National Institute of Standards and Technology (NIST) is leading efforts to standardize Post-Quantum Cryptography (PQC) algorithms to future-proof encryption. Meanwhile, the geopolitical race between nations like China and the U.S. to develop quantum computing capabilities adds another layer of complexity to this emerging threat landscape.



Supply Chain Attacks

SolarWinds Hack (2020)

Attackers compromised SolarWinds' software update system, pushing malicious updates to thousands of customers, including U.S. government agencies. This sophisticated attack remained undetected for months, demonstrating the severe impact of supply chain compromises.

1

MOVEit Transfer Vulnerability (2023)

The Clop ransomware group exploited a zero-day vulnerability in the widely-used MOVEit file transfer software, compromising data from hundreds of organizations globally. This incident underscored the ongoing risk of vulnerabilities in commonly used third-party software.

3

2

Kaseya VSA Ransomware Attack (2021)

The REvil ransomware group exploited vulnerabilities in Kaseya's IT management platform, affecting thousands of businesses worldwide. This attack highlighted how targeting managed service providers can lead to widespread, cascading impacts.

Supply chain attacks continue to pose a significant threat as attackers increasingly target third-party vendors to gain access to multiple victims simultaneously. Mitigation strategies include the adoption of Software Bill of Materials (SBOM), rigorous vendor audits, and continuous monitoring of third-party software. Organizations must also implement robust incident response plans that account for supply chain compromises.

Cloud Threats and Misconfigurations



Cloud Misconfigurations

The 2019 Capital One breach, resulting from a misconfigured AWS firewall, exposed sensitive data of over 100 million customers. This incident highlights how simple misconfigurations can lead to massive data breaches in cloud environments. Organizations must implement robust configuration management and continuous auditing processes to mitigate this risk.



API Vulnerabilities

The 2021 T-Mobile data breach, where attackers exploited an API to steal personal data from 50 million customers, underscores the critical importance of securing APIs in cloud services. As organizations increasingly rely on APIs for inter-service communication, securing these endpoints becomes paramount to overall cloud security.



Mitigation Strategies

Implementing Zero Trust architectures, securing APIs through strong authentication and authorization mechanisms, and leveraging cloud-native security tools are essential strategies. Additionally, organizations should invest in cloud security posture management (CSPM) tools to continuously monitor and remediate misconfigurations.

Internet of Things (IoT) Vulnerabilities



Mirai Botnet (2016)

A devastating DDoS attack leveraging thousands of unsecured IoT devices, highlighting the critical need for IoT security standards. The attack overwhelmed major websites, causing widespread service disruptions and exposing the fragility of our interconnected digital ecosystem.



Insulin Pump Vulnerabilities

Security flaws discovered in connected insulin pumps led to a massive recall, underscoring the life-threatening risks posed by insecure medical IoT devices. This incident sparked urgent discussions about the need for stringent security measures in healthcare technology.



Mitigation Strategies

Implementation of regular firmware updates, network segmentation for IoT devices, and adherence to evolving security standards. These measures are crucial to creating a resilient IoT infrastructure capable of withstanding sophisticated cyber threats.

The proliferation of IoT devices has dramatically expanded the attack surface for cybercriminals. Without robust security measures, these connected devices become potential entry points for malicious actors, threatening both individual privacy and organizational security. As we move forward, it's imperative that manufacturers and users alike prioritize security in the design, deployment, and maintenance of IoT ecosystems.

Mobile Device Threats



Zero-day Vulnerabilities

Zero-day exploits continue to pose significant threats to mobile devices, with sophisticated attackers leveraging undiscovered flaws in operating systems and applications. The Pegasus Spyware case of 2021 exemplifies the potential for these vulnerabilities to be weaponized for surveillance and espionage, targeting journalists and activists with alarming precision.



Mobile Banking Malware

The rise of mobile banking has been accompanied by an increase in specialized malware targeting financial applications. The Anubis Banking Trojan, which targeted Android users in 2019, demonstrates the evolving sophistication of these threats. By mimicking legitimate apps, such malware can steal sensitive financial data and credentials, leading to significant financial losses for individuals and institutions.



Mitigation Strategies

To combat these threats, organizations must implement robust mobile device management (MDM) solutions, enforce regular software updates, and educate users about safe mobile practices. Additionally, the development of AI-driven threat detection systems for mobile platforms is crucial in identifying and neutralizing emerging threats in real-time.

As mobile devices become increasingly central to both personal and professional activities, securing these endpoints is paramount. The dynamic nature of mobile threats requires a proactive and adaptive security approach, combining technological solutions with user awareness and ongoing threat intelligence.

Phishing Trends

The landscape of phishing attacks has become increasingly sophisticated in 2024. Cybercriminals are employing advanced techniques to bypass traditional security measures and exploit human vulnerabilities. One of the most concerning trends is the rise of spear phishing and targeted attacks. These personalized campaigns leverage data mined from social media and other sources to create highly convincing emails tailored to specific individuals or departments.

Another significant development is the widespread use of AI-generated content in phishing emails. These messages mimic human writing styles with uncanny accuracy, making them extremely difficult to detect using conventional methods. Additionally, threat actors are quick to exploit current events and global crises, crafting emotionally charged messages that capitalize on fear and urgency.



Spear Phishing and Targeted Attacks

Personalized campaigns using social media data increase success rates and evade generic filters.



AI-Generated Content

Sophisticated phishing emails mimic human writing, challenging traditional detection methods.



Exploitation of Current Events

Campaigns adapt quickly to news cycles, triggering emotional responses for higher success rates.



Multi-Stage Phishing Attacks

Complex campaigns employ follow-up social engineering calls after initial phishing success.

Business Email Compromise



High-Value Targeting

Business Email Compromise (BEC) attacks have evolved significantly in 2024, focusing on high-value targets and employing more sophisticated techniques. Cybercriminals are now prioritizing senior executives and finance departments, with a particular emphasis on CEO fraud and invoice scams targeting CFOs.



Multi-Faceted Attacks

One of the most alarming trends is the combination of BEC with phishing and social engineering techniques. Attackers initiate contact through phishing emails and then follow up with elaborate social engineering tactics, creating prolonged attack timelines that make detection increasingly challenging.



Cloud Platform Exploitation

Cloud-based email platforms like Microsoft 365 and Google Workspace have become prime targets, with attackers gaining access to email threads to launch highly convincing spoofing attacks.

Zero-Click Exploits No Interaction Required



Vulnerability Identification

Attackers focus on discovering zero-day vulnerabilities within popular messaging apps like WhatsApp and Telegram, as well as the core operating systems of both Android and iOS.



Exploit Development

Sophisticated malware is specifically engineered to exploit these vulnerabilities without requiring any user interaction. This enables attackers to gain control of a device silently, even without the victim clicking a single link or opening a malicious attachment.



Silent Deployment

The malware is deployed via inconspicuous methods like SMS messages that appear as legitimate notifications or alerts. These messages may impersonate trusted sources, such as banks or delivery services, urging users to take immediate action.



Device Compromise

Once the malware is successfully deployed, the attacker gains full control of the victim's device. This includes access to sensitive information stored on the device, such as personal data, financial details, and even the ability to remotely control the device's camera and microphone.

Open Source Infiltration

- **Open Source Risks:** Attackers are increasingly targeting popular open-source projects like npm, PyPI, and even widely used utility libraries such as xz-utils. By inserting backdoors into these projects, attackers can infiltrate the software supply chain and spread malicious code. This exposes downstream projects and users relying on compromised software to a range of threats, from data breaches to remote code execution.
- **The xz-utils Breach of 2023:** This attack was particularly unique because it targeted a widely trusted open-source project, xz-utils, which is a fundamental component used across numerous Linux systems and distributions. Unlike typical attacks that exploit existing vulnerabilities, the attackers cleverly gained unauthorized access to the code repository itself and subtly inserted the backdoor, embedding malicious code directly into the development process. This type of supply chain infiltration is rare and highly sophisticated, as it bypasses traditional security defenses by embedding the vulnerability at the source. The breach was only discovered through a proactive code audit, highlighting both the unusual nature of the attack and the challenges in detecting such sophisticated threats. It underscored how deeply ingrained vulnerabilities can become when they are introduced into trusted open-source software that is widely distributed across industries.
- **Mitigation Strategies:** To counter this threat, developers and organizations must prioritize security practices throughout the open-source software lifecycle. These include regular code audits, use of automated security tools, thorough dependency tracking, prompt patching of vulnerabilities, and continuous monitoring of open-source projects and software updates.



Healthcare Sector Threats



Ransomware Attacks

Healthcare providers are prime targets for ransomware due to the critical nature of their services and the sensitivity of patient data. The Ryuk ransomware attack in 2019 caused significant operational disruptions, highlighting the sector's vulnerability.



Legacy Systems

Many healthcare institutions rely on outdated software and systems, creating security vulnerabilities. The WannaCry attack in 2017 exploited these weaknesses in the UK's NHS, causing widespread disruptions to patient care.



Medical IoT Risks

Connected medical devices like pacemakers and insulin pumps present unique security challenges. The 2017 pacemaker vulnerabilities case led to the recall of over 465,000 devices, underscoring the life-threatening potential of IoT security flaws in healthcare.



Data Breaches

Healthcare data breaches can have severe consequences, including identity theft and compromised patient care. Stringent regulations like HIPAA in the US aim to protect patient data, but breaches remain a persistent threat.

The healthcare sector faces a unique combination of cyber threats, balancing the need for technological advancement with the imperative of protecting sensitive patient data and ensuring uninterrupted care. As healthcare becomes increasingly digitized, robust cybersecurity measures and staff training are crucial to safeguarding this critical infrastructure.

Cybersecurity Trends for 2024 and Beyond



Quantum Computing

Advancements in quantum computing pose significant risks to current encryption standards. Simulations of Shor's Algorithm demonstrate the potential to break RSA-2048 encryption rapidly, necessitating the development and implementation of quantum-resistant cryptographic algorithms.



AI-Driven Defenses

The integration of AI in cybersecurity is accelerating, with machine learning algorithms enhancing threat detection and response capabilities. AI-powered Security Operations Centers (SOCs) have shown promising results, significantly reducing response times to cyber threats.



Evolving Regulations

Global privacy regulations like GDPR and CCPA are setting new standards for data protection. The EU's NIS2 Directive focuses on critical infrastructure protection, signaling a trend towards more comprehensive and stringent cybersecurity regulations worldwide.



Zero Trust Architecture

The adoption of Zero Trust security models is becoming essential, particularly in the era of remote work. This approach, which assumes no trust and verifies every access request, is critical for protecting distributed networks and cloud-based resources.

As we look towards the future of cybersecurity, organizations must stay ahead of these emerging trends. Investing in quantum-resistant encryption, leveraging AI for enhanced security, ensuring regulatory compliance, and implementing Zero Trust architectures will be crucial for maintaining robust cybersecurity postures in an increasingly complex threat landscape.

Executive Summary



Key Takeaways

The cybersecurity landscape of 2024 is characterized by sophisticated threats from nation-state actors, evolving ransomware tactics, and unprecedented privacy challenges. IoT vulnerabilities, mobile device threats, and healthcare sector risks underscore the need for comprehensive security strategies across all industries.



Actionable Strategies

Organizations must prioritize the adoption of Zero Trust architectures, invest in AI-driven defense systems, and strengthen vendor risk management practices. Implementing robust data protection measures, conducting regular security audits, and fostering a culture of cybersecurity awareness are crucial steps in mitigating emerging threats.



Next Steps

Immediate action is required to strengthen security frameworks, monitor emerging technologies like quantum computing, and ensure compliance with evolving regulations. Continuous education and training for staff, coupled with investments in cutting-edge security technologies, will be essential for maintaining resilience in the face of evolving cyber threats.

The rapidly evolving cybersecurity landscape demands a proactive and adaptive approach. By implementing these strategies and maintaining vigilance against emerging threats, organizations can enhance their security posture and protect their critical assets in an increasingly complex digital environment. The time for action is now – cybersecurity must be at the forefront of every organization's strategic planning to ensure long-term resilience and success.

Questions?

Contact:

CSOCTI@HHS.GOV



FTC Health Privacy Update



Ryan Mehm
Division of Privacy and Identity Protection
Federal Trade Commission

The views expressed are those of the speaker
and not necessarily those of the FTC

FTC Background



- Independent law enforcement agency
- 2-part mandate:
 - Consumer protection
 - Competition
- Privacy and data security are consumer protection priorities
 - Enforcement
 - Policy initiatives
 - Consumer education and business outreach

FTC Background



Authority: FTC Act

“Unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.”

*Federal Trade Commission Act,
Section 5 (15 U.S.C. § 45)*

FTC Act Fundamentals



- **Deception**

- A material representation or omission that is likely to mislead consumers acting reasonably under the circumstances

- **Unfairness**

- A practice that causes or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers

HIPAA & the FTC Act



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

- Section 5 authority extends to both HIPAA and non-HIPAA covered entities
- OCR and FTC enforce sister health breach notification rules
- Joint Guidance (Aug. 2024): [Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule](#)
- Joint cases: CVS and Rite Aid

Health Breach Notification Rule (HBNR)

- Rule requires notification of the breach of unsecured identifiable health information in personal health records (PHRs) to individuals, FTC, and (in some cases) the media
- Applies to:
 - Vendors of personal health records (PHRs)
 - PHR related entities
 - Third party service providers

HBNR Final Rule Amendments

- Amendments consistent with public comments and Commission's September 2021 policy statement, which underscored how the Rule applies to:
 - health apps
 - unauthorized disclosures (not just cybersecurity incidents)
- Amendments went into effect on July 29, 2024

Health Breach Notification Rule Amendments

- Eight Main Take-aways:
 - #1: Rule applies to health apps and similar technologies not covered by HIPAA
 - #2: Breach includes data security breaches + unauthorized disclosures
 - #3: Clarification regarding what it means to draw PHR identifiable health information from multiple sources
 - #4: Revised definition of “PHR related entity”
 - #5: Expanded use of electronic notice to consumers
 - #6: Expanded content of notice to consumers
 - #7: Altered timing requirement for notice to FTC
 - #8: Added cross-references, citations, and more information about penalties for non-compliance

Health Breach Notification Rule Updated Business Guidance

- [Health Breach Notification Rule: The Basics for Business](#)
- [Complying with the FTC's Health Breach Notification Rule](#)
- [Mobile Health App Tool](#)
- [Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule](#)

Health Breach Notification Rule: How to Report a Breach to the FTC

- Use the online form: [Notice of Breach of Health Information](#)
 - Form will request information about:
 - Your company or organization;
 - The breach; and
 - Your breach notification
 - After completing form, you should receive a reply email within two to five business days with instructions to securely submit documents (e.g., copy of notice sent to affected individuals) related to the breach

Monument

- Alcohol addiction treatment service shared consumers' health data for advertising purposes with third parties, contrary to promises and without consumer consent
- Complaint alleges:
 - Deceived users about sharing practices with third parties
 - Misrepresented HIPAA compliance
 - Violated OARFPA by misrepresenting its practices regarding disclosure of users' personal information, including health information, and disclosing information without consent
- First privacy enforcement action alleging violations of Opioid Addiction Recovery Fraud Prevention Act of 2018 (OARFPA)
- FTC jurisdiction extends to HIPAA-covered entities

Cerebral and BetterHelp

- Cerebral
 - Mental health and pain management subscription service turned over sensitive health data of nearly 3.2 million consumers to third parties, including LinkedIn, Snapchat, and TikTok
- BetterHelp
 - Mental health and telehealth counseling service allegedly shared personal information with third parties for advertising without consent and contrary representations to consumers

GoodRx and Easy Healthcare Corp. (Premom)

- Premom
 - Fertility app allegedly shared users' personal information with third parties, including two China-based firms, and failed to notify consumers
- GoodRx
 - Telehealth and discount drug provider allegedly shared personal information with third parties for advertising without consent and contrary to representations
 - Complaint alleges GoodRx failed to notify consumers and FTC of unauthorized disclosures of health info to third parties for advertising
- First HBNR enforcement actions

Joint FTC-HHS Letters

- July 2023 letters to 130 hospital systems and telehealth providers
- Cautions them about the privacy and security risks related to the use of online tracking technologies, which may disclose consumers' sensitive personal health data to third parties
- Highlights that this tech gathers identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid

Security of Health Information

- **Vitagene** – Alleged that genetic testing firm claimed to exceed industry-standard security practices, while storing health and DNA information in plain text in publicly accessible cloud repositories
- **Premom** - Alleged that app developer didn't employ reasonable security, including by failing to assess the risks of third-party SDKs
- **Chegg** - Alleged that ed tech provider failed to protect personal information collected from users and employees, resulting in exposure through 4 data breaches of health, financial, and other information of millions
- **SkyMed** – Alleged that emergency travel services provider failed to take reasonable measures to secure sensitive data, including health records

Remedies

- Ban on disclosing health information for advertising
- Third Party Deletion
- Privacy Programs
- Security Programs
- Notice to Consumers
- Money
 - Penalties
 - Consumer redress

Takeaways

- What is health information?
- Risks associated with ad tech
- DTC tech – apps, telehealth, genetic testing
- HIPAA claims
- Biometric data
- Using every tool in the toolbox
- Serious consequences for violating Section 5, HBNR, and OARFPA
 - Ban on sharing health data for advertising
 - \$\$\$

Education

- [Protecting the privacy of health information: A baker's dozen takeaways from FTC cases](#)
- [Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking](#)
- [The DNA of privacy and the privacy of DNA](#)
- [Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data](#)
- [Mobile Health App Tool](#)
- [Health Breach Notification Rule: The Basics for Business](#)
- [Complying with the FTC's Health Breach Notification Rule](#)

Questions?

Ryan Mehm
Federal Trade Commission
rmehm@ftc.gov

FDA's Medical Device Cybersecurity Policies and Programs

Jessica Wilkerson

Senior Cyber Policy Advisor and Medical Device Cybersecurity Team Lead
Division of Medical Device Cybersecurity (DMDC)
Office of Resilience and Response (ORR)
Office of Strategic Partnerships and Technology Innovation (OST)
Center for Devices and Radiological Health (CDRH)
Food and Drug Administration
jessica.wilkerson@fda.hhs.gov



The “Why:” Cyber Threats to the Healthcare Sector

The “Why:” Cyber Threats to the Healthcare Sector

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

[f Share](#) [t Tweet](#) [in LinkedIn](#) [✉ Email](#) [🖨 Print](#)

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers, and manufacturers about the SweynTooth family of cybersecurity vulnerabilities, which may introduce risks for certain medical devices. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. Software to exploit these vulnerabilities in certain situations is already publicly available.

The “Why:” Cyber Threats to the Healthcare Sector

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

[f Share](#) [t Tweet](#) [in LinkedIn](#) [✉ Email](#) [🖨 Print](#)

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers, and manufacturers about the SweynTooth family of cybersecurity vulnerabilities, which may introduce risks for certain medical devices. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. Software to exploit these vulnerabilities in certain situations is already publicly available.

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication

[f Share](#) [t Tweet](#) [in LinkedIn](#) [✉ Email](#) [🖨 Print](#)

Date Issued: January 23, 2020

The “Why:” Cyber Threats to the Healthcare Sector

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

[Share](#) [Tweet](#) [LinkedIn](#) [Email](#) [Print](#)

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers, and manufacturers about the SweynTooth family of cybersecurity vulnerabilities, which may introduce risks for certain medical devices. The FDA is aware of any confirmed adverse events related to these vulnerabilities. Software updates to address these vulnerabilities in certain situations is already publicly available.

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication

[Share](#) [Print](#)

Illumina Cybersecurity Vulnerability Affecting the Universal Copy Service Software May Present Risks for Patient Results and Customer Networks: Letter to Health Care Providers

[Share](#) [Tweet](#) [LinkedIn](#) [Email](#) [Print](#)

The “Why:” Cyber Threats to the Healthcare Sector

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication

St. Jude admits security vulnerabilities in cardiac devices

The U.S. Food and Drug Administration (FDA) has advised health care providers to be aware of these vulnerabilities in cardiac devices. After suing the two companies who claimed St. Jude devices had severe vulnerabilities that put patients at risk, the organization released security patches for the devices this week.

By [Jessica Davis](#) | January 10, 2017 | 01:20 PM

[f](#) [t](#) [in](#) [✉](#)

Illumina Cybersecurity Vulnerability Affecting the Universal Copy Service Software May Present Risks for Patient Results and Customer Networks: Letter to Health Care Providers

[f](#) [t](#) [in](#) [✉](#) [Print](#)

[Print](#)

The “Why:” Cyber Threats to the Healthcare Sector

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication

St. Jude admits security vulnerabilities in cardiac devices

Illumina Cybersecurity Vulnerability Affecting the Universal Copy Service Software May Present Risks for Patient Results and Customer Networks: Letter to Health Care Providers

The U
provid
vulner
aware
these

After suing the two companies who claimed St. Jude devices had severe vulnerabilities that put patients the organization this week.

By [Jessica Davis](#) | J

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology

Healthcare & Pharmaceuticals | Data Privacy | Health

FDA warns of cybersecurity risk with certain Medtronic insulin pumps

Reuters

September 21, 2022 4:00 PM EDT · Updated 10 months ago

Print

The “Why:” Cyber Threats to the Healthcare Sector

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication

St. Jude admits security vulnerabilities in cardiac devices

Illumina Cybersecurity Vulnerability Affecting the Universal Copy Service Software May Present Risks for Patient Results and Customer Networks: Letter to Health Care Providers

The U
provid
vulner
aware
these

After suing the two companies who claimed St. Jude devices had severe vulnerabilities that put patients the organization this week.

By **Jessica Davis** | J

REUTERS® World Business Markets Sustainability Legal Breakingviews Technol

Healthcare & Pharmaceuticals | Data Privacy | Health

FDA warns of cybersecurity risk with certain Medtronic insulin pumps

Reuters

September 21, 2022 4:00 PM EDT · Updated 10 months ago

ICS MEDICAL ADVISORY

Fresenius Kabi Agilia Connect Infusion System (Update A)

Last Revised: January 27, 2022 Alert Code: ICSMA-21-355-01

1. EXECUTIVE SUMMARY

- CVSS v3 7.5
- ATTENTION:** Exploitable remotely/low attack complexity
- Vendor: Fresenius Kabi
- Equipment: Agilia Connect Infusion System

The “Why:” Cyber Threats to the Healthcare Sector

YNHHS pauses radiotherapy treatment for six days after software breach

A nationwide cybersecurity threat to Elekta, a vendor that delivers radiotherapy services at the Yale New Haven Health System, resulted in the interruption of treatment for approximately 200 cancer patients for six days.

MARIA FERNANDA PACHECO & RAZEL SUANSING | 10:39 PM, APR 27, 2021
STAFF REPORTERS



Marisa Peryer, Senior Photographer

Vulnerabilities May Affect Safety

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication

Illumina Cybersecurity Vulnerability Affecting the Universal Copy Service Software May Present Risks for Patient Results and Customer Networks: Letter to Health Care Providers

Print

By Jessica Davis | J

Healthcare & Pharmaceuticals | Data Privacy | Health

FDA warns of cybersecurity risk with certain Medtronic insulin pumps

Reuters

September 21, 2022 4:00 PM EDT · Updated 10 months ago

ICS MEDICAL ADVISORY

Fresenius Kabi Agilia Connect Infusion System (Update A)

Last Revised: January 27, 2022

Alert Code: ICSMA-21-355-01

1. EXECUTIVE SUMMARY

- CVSS v3 7.5
- ATTENTION:** Exploitable remotely/low attack complexity
- Vendor: Fresenius Kabi
- Equipment: Agilia Connect Infusion System

The “Why:” Cyber Threats to the Healthcare Sector

YNHHS pauses radiotherapy treatment for six days after software breach

A nationwide cybersecurity threat to Elekta, a vendor that delivers radiotherapy services at the Yale New Haven Health System, resulted in the interruption of treatment for approximately 200 cancer patients for six days.

MARIA FERNANDA PACHECO & RAZEL SUANSING | 10:39 PM, APR 27, 2021
STAFF REPORTERS



Marisa Peryer, Senior Photographer

CommonSpirit cyberattack spurs IT outages at CHI Memorial, hospitals across US

Jessica Davis | October 5, 2022



A cyberattack struck one of the largest nonprofit health systems in the U.S., CommonSpirit Health, and is causing IT disruptions at multiple subsidiary hospitals across the U.S. (Photo Credit: “Emergency room” by KOMUnews is licensed under CC BY 2.0.)

vulnerabilities in Certain GE Information Central Entry Servers: Safety notification

Print

Healthcare & Pharmaceuticals | Data Privacy | Health

FDA warns of cybersecurity risk with certain Medtronic insulin pumps

Reuters

September 21, 2022 4:00 PM EDT · Updated 10 months ago

Last Revised: January 27, 2022

Alert Code: ICSMA-21-355-01

1. EXECUTIVE SUMMARY

- CVSS v3 7.5
- ATTENTION: Exploitable remotely/low attack complexity
- Vendor: Fresenius Kabi
- Equipment: Agilia Connect Infusion System

The "Why:" Cyber Threats to the Healthcare Sector

YNHHS pauses radiotherapy treatment for six days after software breach

A nationwide cybersecurity threat to Elekta, a vendor that delivers services at the Yale New Haven Health System, resulted in the treatment for approximately 200 cancer patients for six days.

MARIA FERNANDA PACHECO & RAZEL SUANSING | 10:39 PM, AP
STAFF REPORTERS



Marisa Peryer, Senior Photographer

CommonSpirit cyberattack spurs IT outages at CHI Memorial, hospitals

Scripps enters fourth week of ransomware attack



View of Scripps Memorial Hospital in Hillcrest on May 3. (Sandy Huffaker/SDUT)

BREAKING >

PUBLIC SAFETY
Woman arrested on suspicion of shooting, killing man in Encanto
Nov. 7, 2022

NATIONAL BUSINESS
Winning numbers for \$2.04B Powerball draw



A cyberattack struck one of the largest nonprofit health systems in the U.S., CommonSpirit Health, and is causing IT disruptions at multiple subsidiary hospitals across the U.S. (Photo Credit: "Emergency room" by KOMUnews is licensed under CC BY 2.0)

abilities in Certain GE Information Central entry Servers: Safety nification

ing ail Print

mer S

Agilia Connect Infusion System

By Jessica Davis | J

Healthcare & Pharmaceuticals | Data Privacy | Health

FDA warns of cybersecurity risk with certain Medtronic insulin pumps

Reuters

September 21, 2022 4:00 PM EDT · Updated 10 months ago

Last Revised: January 27, 2022

Alert Code: ICSMA-21-355-01

1. EXECUTIVE SUMMARY

- CVSS v3 7.5
- ATTENTION:** Exploitable remotely/low attack complexity
- Vendor:** Fresenius Kabi
- Equipment:** Agilia Connect Infusion System

The “Why:” Cyber Threats to the Healthcare Sector

YNHHS pauses radiotherapy treatment for six days after software breach

A nationwide cybersecurity threat to Elekta, a vendor that delivers radiotherapy services at the Yale New Haven Health System, resulted in the interruption of treatment for approximately 200 cancer patients for six days.

MARIA FERNANDA PACHECO & RAZEL SUANSING | 10:39 PM, APRIL 14, 2022
STAFF REPORTERS



Marisa Peryer, Senior Photographer

CommonSpirit cyberattack spurs IT outages at CHI Memorial, hospitals

Scripps enters fourth week of ransomware attack



View of Scripps Memorial Hospital in Hillcrest on May 3. (Sandy Huffaker/SDUT)

Weaknesses in Certain GE Information Central Systems May Pose Safety Risks

Critical flaws found in interoperability backbone: FHIR APIs vulnerable to abuse

Jessica Davis | October 13, 2021



Interoperability and greater data sharing across health care is a top priority of HHS, but its reliance on APIs pose some privacy and security risks. Medical staff analyze patient data at the Department of Rehabilitative Cardiology of ASL 3 Genova on July 21, 2020, in Genova, Italy. (Photo by Marco Di Lauro/Getty Images)

By Jessica Davis | J

Healthcare & Pharmaceuticals | Data Privacy | Health

FDA warns of cybersecurity risk to certain Medtronic insulin pumps

Reuters

September 21, 2022 4:00 PM EDT · Updated 10 months ago

A cyberattack struck one of the largest nonprofit subsidiary hospitals across the U.S. (Photo Credit: [unreadable])

BREAKING >

PUBLIC SAFETY

Woman arrested on suspicion of shooting man in Encanto
Nov. 7, 2022

NATIONAL BUSINESS

Winning numbers for \$2.04B Powerball
Nov. 7, 2022

- ATTENTION: Exploitable remotely/low attack complexity
- Vendor: Fresenius Kabi
- Equipment: Agilia Connect Infusion System

The “Why:” Cyber Threats to the Healthcare Sector

YNHHS pauses radiotherapy treatment for six days after software breach

A nationwide cybersecurity threat to Elekta, a vendor that delivers radiotherapy services at the Yale New Haven Health System, resulted in the interruption of treatment for approximately 200 cancer patients for six days.

MARIA FERNANDA PACHECO & [...] STAFF REPORTERS



By Jessica Davis

CommonSpirit cyberattack spurs IT outages at CHI Memorial, hospitals

Scripps enters fourth week of ransomware attack

abilities in Certain GE Information Central Safety

Cyber threats can, have, and do pose patient safety risks to the healthcare sector

certain Medtronic insulin pumps

Reuters

September 21, 2022 4:00 PM EDT · Updated 10 months ago

Interoperability and greater data sharing across health care is a top priority of HHS, but its reliance on APIs pose some privacy and security risks. Medical staff analyze patient data at the Department of Rehabilitative Cardiology of ASL 3 Genova on July 21, 2020, in Genoa, Italy. (Photo by Marco Di Lauro/Getty Images)

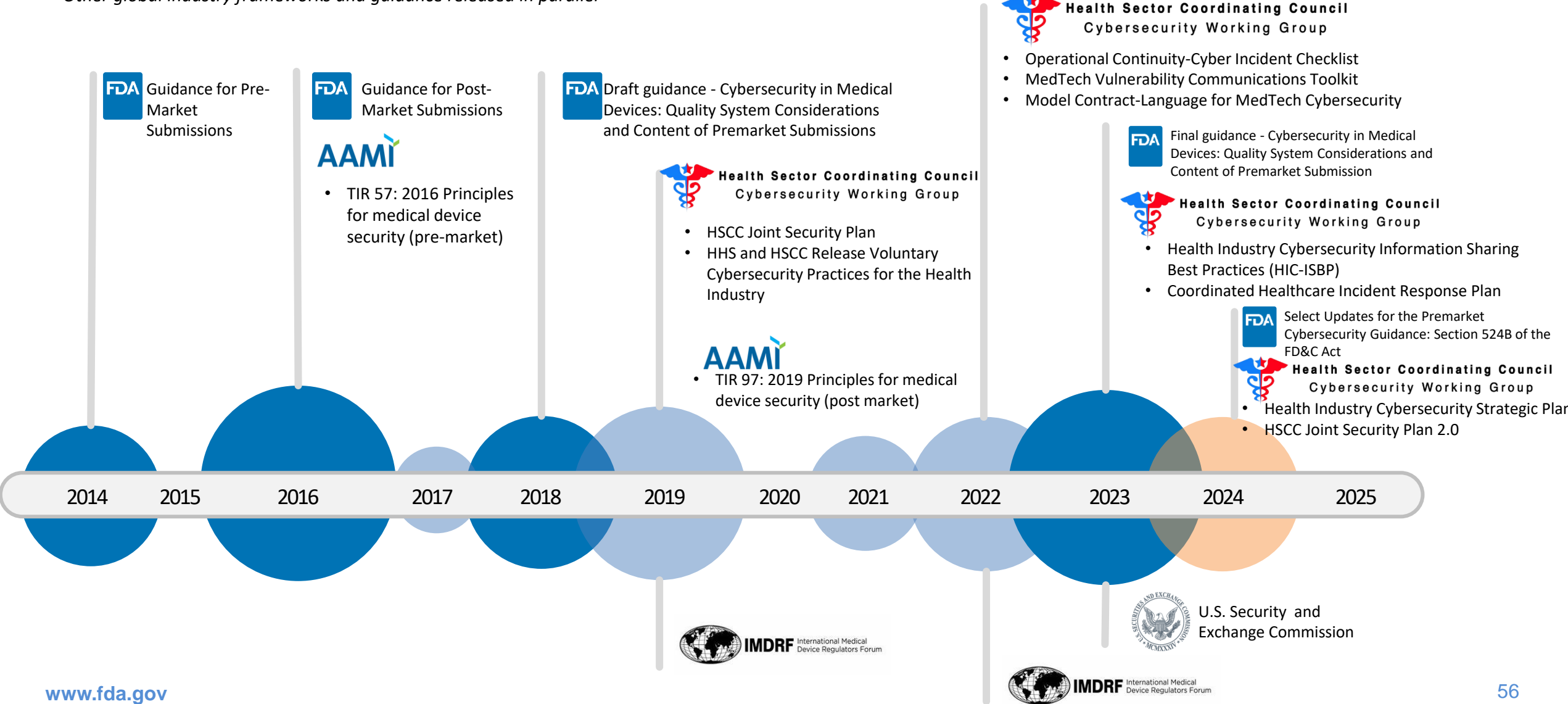


- ATTENTION: Exploitable remotely/low attack complexity
- Vendor: Fresenius Kabi
- Equipment: Agilia Connect Infusion System

on System

Medical Device cybersecurity landscape

Other global industry frameworks and guidance released in parallel



FD&C ACT SECTION 524B – ENSURING CYBERSECURITY OF MEDICAL DEVICES



Section 524B of FD&C Act

- The Consolidated Appropriations Act for 2023 was signed into law December 29, 2022 and includes the Food and Drug Omnibus Reform Act (FDORA)
- [Section 3305](#) of Omnibus – Ensuring Cybersecurity of Medical Devices
- Adds New Section 524B of the FD&C Act – Ensuring Cybersecurity of Devices
- Applies to prospective submissions for ‘cyber devices’ under the 510(k), de Novo, HDE, PDP, and PMA pathways
- Effective 90 days after signing (March 29, 2023)

524B(c) - Cyber Device

Section 524B(c) defines a Cyber Device as a device that:

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

524B Requirements

- Section 524B(a) requires that a sponsor of an application (of the aforementioned submission types) provide the documentation required described in subsection (b)
- Section 524B(b) requires manufacturers of cyber devices to:
 1. Submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures;
 2. Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecurity, and make available postmarket 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;
 3. Provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and
 4. Comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecurity

FDA Final Premarket Guidance



- [Published](#) on September 26, 2023
- Recommendations are intended to help manufacturers comply with requirements under Section 524B of the FD&C Act
- Addresses how cybersecurity fits into the Quality System Requirements (21 CFR Part 820) and premarket submission documentation requirements
- [Public Webinar](#) on November 2, 2023
- eSTAR will include a guided walk-through of the guidance (and 524B) to inform/support electronic submissions

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Draft Premarket Select Update

- [Published](#) on March 12, 2024
 - Interpretations of key terms
 - Premarket submission documentation for each 524B requirement
 - Premarket submission documentation for modifications to existing devices
 - Interpretation of how 524B fits into existing regulatory submission criteria
- When finalized, will be added to Final Premarket Cybersecurity Guidance
- [Public Webinar](#) will be held on April 30, 2024

Contains Nonbinding Recommendations

Draft – Not for Implementation

**Select Updates for the Premarket
Cybersecurity Guidance: Section 524B
of the FD&C Act**

**Draft Guidance for Industry and
Food and Drug Administration Staff**

DRAFT GUIDANCE


This draft guidance document is being distributed for comment purposes only.

Document issued on March 13, 2024.

You should submit comments and suggestions regarding this draft document within 60 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to <https://www.regulations.gov>. Submit written comments to the Dockets Management Staff, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852-1740. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions about this document regarding CDRH-regulated devices, contact CDRHManufacturerShortage@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

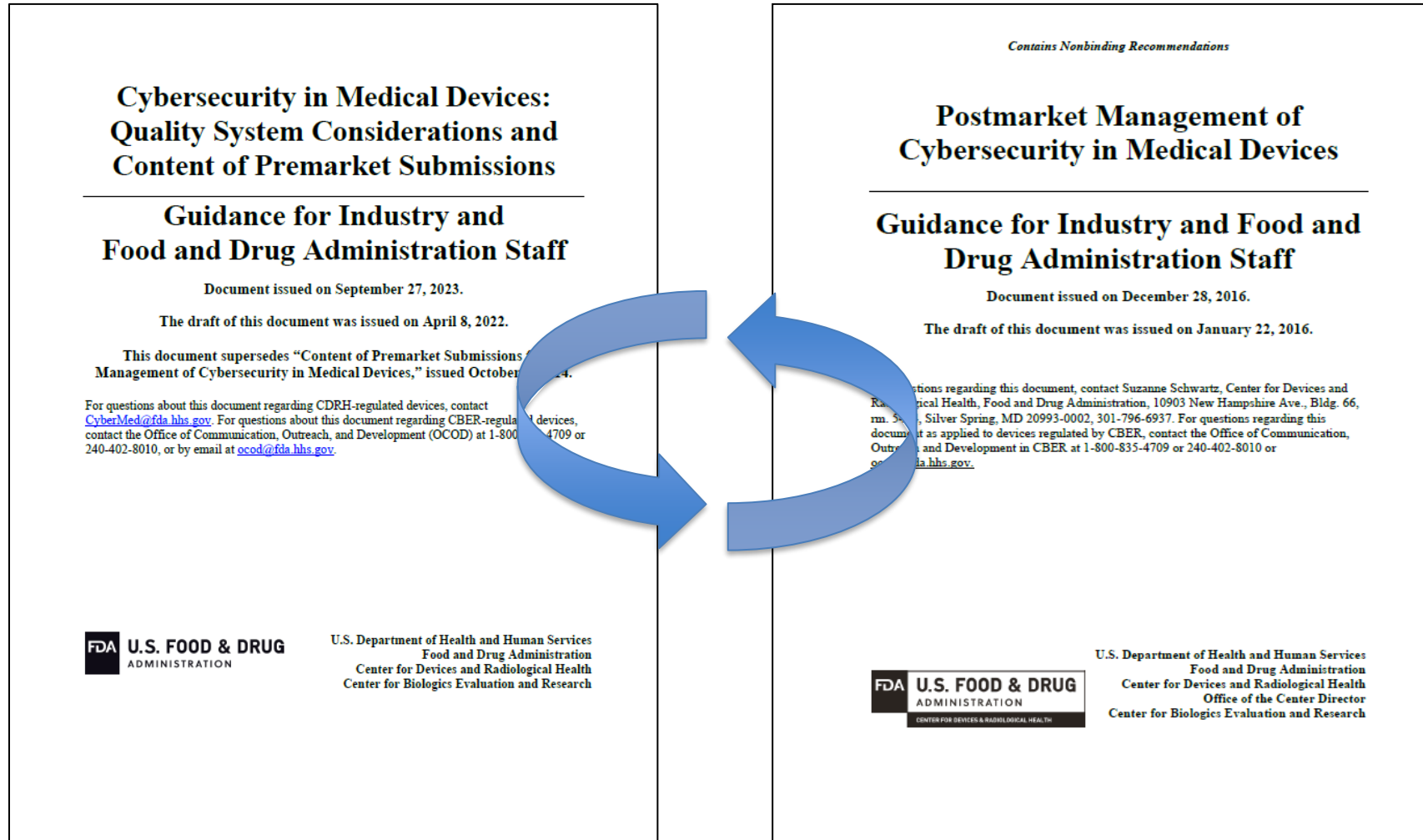
When final, this guidance will supersede “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions,” issued September 27, 2023.



**U.S. FOOD & DRUG
ADMINISTRATION**

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

FDA Final Cybersecurity Guidance




Premarket Reviews Today



Guidance for Industry
Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
Document issued on: January 14, 2005

For questions regarding this document contact John F. Murray Jr. 240-276-0284, john.murray@fda.hhs.gov.



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Compliance
Office of Device Evaluation

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions
Guidance for Industry and Food and Drug Administration Staff
Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact OCOD@fda.hhs.gov.

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.


For questions about this document regarding CDRH-regulated devices, contact the Division of Digital Health at DigitalHealth@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov. For questions about this document regarding CDRH-regulated combination products, contact the Center for Drug Evaluation and Research, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 51, Rm. 6158, Silver Spring, MD 20993-0002, 301-796-8936. For questions about this document regarding combination products, contact the Office of Combination Products at combination@fda.gov.

Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices
Guidance for Industry and Food and Drug Administration Staff
Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research


Contains Nonbinding Recommendations

Content of Premarket Submissions for Device Software Functions
Guidance for Industry and Food and Drug Administration Staff
Document issued on June 14, 2023.

The draft of this document was issued on November 4, 2021.

This document supersedes Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 2005.

For questions about this document regarding CDRH-regulated devices, contact the Digital Health Center of Excellence at digitalhealth@fda.hhs.gov. For questions about this document regarding CBER regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research
Center for Drug Evaluation and Research
Office of Combination Products in the Office of the Commissioner


Contains Nonbinding Recommendations

Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices
Guidance for Industry and Food and Drug Administration Staff
Document issued on: September 6, 2017

The draft of this document was issued on January 26, 2016.

For questions about this document regarding CDRH-regulated devices, email them to: DigitalHealth@fda.hhs.gov.

For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 240-402-8010.




U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Contains Nonbinding Recommendations

Off-The-Shelf Software Use in Medical Devices
Guidance for Industry and Food and Drug Administration Staff
Document issued on September 27, 2019.

Document originally issued on September 9, 1999.

For questions about this document, contact the Division of Digital Health by e-mail at digitalhealth@fda.hhs.gov.



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health

Services
Health
Search
Research
Consumer

Cybersecurity Reviews



- “... software engineering is about *ensuring that certain things happen ...*, **security is about ensuring that they don’t**”¹
- What can the device do or be made to do versus what was it designed to do?
- Past Performance \neq Future Security
- ~~“Who is ever going to do that?”~~



Does Cybersecurity Apply?

- Cybersecurity applies if the device is or contains software
- Cybersecurity documentation is required if the device meets the definition of a Cyber Device
- Cybersecurity considerations apply regardless of whether the software or software component was designed by the medical device manufacturer or a third-party
- Risks **increase** if device contains one or more of these example interfaces:
 - Wired: USB, ethernet, SD, CD, RGA, etc. or
 - Wireless: Wi-Fi, Bluetooth, RF, inductive, Cloud, etc.
- Cybersecurity considerations apply for entire system, not just end device. Examples include:
 - Software update infrastructure
 - Cloud applications
 - Commercial devices (phones, tablets, computers, etc.)

Guidance Documentation for Reviews



Security Risk Management



Security Architecture



Cybersecurity Testing



Labeling



Cybersecurity Management Plan

Security Risk Management



Threat Modeling



Cybersecurity Risk Assessment



Interoperability



Third-Party Software Components (SBOM)



Unresolved Anomalies



TPLC Security Risk Management (Metrics)

Guidance Documentation for Reviews



Security Architecture

- Implementation of Security Controls
 - Security needs to be designed in
 - 8 Control Categories
 - Appendix 1 contains recommendations for each category
- Architecture Views
 - 4 Types of Views
 - Global System View
 - Multi-Patient Harm View
 - Updateability/Patchability View
 - Security Use Case View(s)
 - Appendix 2 contains recommendations for the level of detail for the views

Cybersecurity Premarket Reviews – What if the Review Concludes the Device’s Cybersecurity is Inadequate?



- If a reviewer determines that a device’s cybersecurity is inadequate, the reviewer will communicate with the submitting MDM (the “sponsor”) to address the identified issues.
- This may involve the use of [deficiencies](#), or requests for additional information needed to make a decision on a medical device marketing application.
- A deficiency generally involves the following four elements:
 - What did the MDM include?
 - What was wrong or missing from the MDM’s submission?
 - Why does FDA need the requested information to appropriately evaluate the device’s safety and effectiveness?
 - What should the MDM do to resolve the issue?

What Does FDA Do When There is a Medical Device Cybersecurity Vulnerability or Incident?



- Medical devices and the manufacturers who produce them demonstrably experience cybersecurity vulnerabilities and incidents
- In certain cases, the vulnerabilities may present a “**controlled**” risk, such that they may be fixed as part of routine updates
- In other cases, the vulnerabilities may present an “**uncontrolled**” risk to patient safety, and must be addressed quickly
- FDA routinely works with MDMs, CISA, Health-ISAC, and others (which now includes VHA!) to assess risks, evaluate mitigations, and inform stakeholders (including the public) about risk
 - See FDA CDRH’s [Cybersecurity page](#), which includes our Safety Communications related to cybersecurity vulnerabilities or incidents

Key Takeaways

- Medical device cybersecurity is part of FDA's overall mandate to protect and promote the public health
- Our statute now explicitly includes cybersecurity requirements that medical device manufacturers must meet
- FDA has a Division of Medical Device Cybersecurity, and device cybersecurity is integrated throughout the agency's operations
- We monitor for, respond to, and learn from device cybersecurity incidents to improve the way we regulate
- Our partnerships with agencies like VHA, OCR, and NIST are a key part of that

QUESTIONS?



U.S. FOOD & DRUG
ADMINISTRATION

Medical Internet of Things and IoT Cybersecurity Panel

Panelists

- **Katerina Megas** (Moderator), NIST Cybersecurity for IoT Program Director
- **Jessica Wilkerson**, FDA Senior Cyber Policy Advisor
Division of Medical Device Cybersecurity
- **Mike Fagan**, NIST Cybersecurity for IoT Technical Lead
- **Connor Walsh**, Veterans Health Administration (VHA)
Medical Device Networking and Cybersecurity Director
- **Nick Heesters**, HHS Office for Civil Rights (OCR) Senior
Advisor for Cybersecurity

Related Resources

FDA

- [Cybersecurity | FDA](#)

HHS OCR

- [HIPAA Security Rule Guidance](#)
- HIPAA Security Rule Videos:
 - <https://www.youtube.com/@USGovHHSOCR>
 - <https://www.youtube.com/watch?v=VnbBxxyZLc8>

VHA

- VHACOHTMNETWORKINGCYBERSECURITY@va.gov

NIST

- [NIST Cybersecurity for IoT Program](#)