

## Cylera Support for HHS CPGs

# Align Healthcare Security Practices with HHS Cyber Performance Goals

Real-time, automated assessment of HHS CPGs and guidance for further strengthening cyber defenses



## The Challenge

Cyber attacks are an increasing threat to the U.S. Health and Public Health (HPH) sector. These attacks can directly compromise secure healthcare delivery and patient safety.

In response to the proliferation of connected medical devices and the rapidly expanding cyber threat landscape, in January 2024 the U.S. Department of Health and Human Services (HHS) released voluntary, healthcare-specific Cybersecurity Performance Goals (CPGs).

HHS CPGs directly address common attack vectors against U.S. hospitals. However, many health systems are still working to understand how to align with the new CPGs. Lack of funding and resources also present challenges. A more automated, streamlined approach to measuring current conformance with HHS CPGs is needed.

## The Solution



Cylera provides the easiest, most accurate, and extensible platform for healthcare IoT intelligence and security. The platform was specifically designed for Healthcare Delivery Organizations (HDOs) who must optimize cyber defenses across healthcare IT, IoT, connected medical devices, and building management systems.

The Cylera platform provides comprehensive asset discovery and inventory, vulnerability and risk management, threat detection and response, network segmentation and protection, and analytics and reporting. It also provides coverage for common healthcare compliance regulations and guidelines, including support for HHS CPGs.

## Benefits

- ▶ Demonstrate alignment with security controls included in the HHS CPGs, as well as with other healthcare industry cybersecurity standards and regulations
- ▶ Provide robust device discovery and inventory uniquely suited for healthcare environments
- ▶ Utilize advanced healthcare IoT vulnerability and risk management capabilities
- ▶ Detect anomalies and threats in real-time, then quickly respond with built-in, detailed remediation guidance
- ▶ Integrate with firewall and network access control (NAC) solutions to help enable network segmentation and zero trust
- ▶ Provide flexible dashboards and reports for cyber risk monitoring
- ▶ Leverage extensive integrations with other systems to improve operational efficiency

## Representative Examples of Cylera HHS CPG Support

| Essential CPGs                                                                        |                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mitigate Known Vulnerabilities                                                        | The Cylera platform enables organizations to take a risk-based vulnerability management approach for all healthcare IoT devices by identifying, validating, and prioritizing vulnerabilities based on their likelihood of exploitability.                                                                                                    |
| Basic Cybersecurity Training                                                          | Cylera provides healthcare IoT and connected medical device cybersecurity training for customer security and biomedical teams as a part of the support package included with the purchase of the Cylera platform.                                                                                                                            |
| Basic Incident Planning and Preparedness                                              | The Cylera platform provides robust incident identification capabilities and detailed remediation guidance for threats specific to healthcare devices across vendors, enabling response teams to remediate incidents swiftly.                                                                                                                |
| Separate User and Privileged Accounts                                                 | The Cylera platform provides a separation of duties model and role-based user access controls to prevent threat actors from accessing privileged accounts when common user accounts are compromised.                                                                                                                                         |
| Vendor/Supplier Cybersecurity Requirements                                            | The Cylera platform captures comprehensive healthcare IoT and connected medical device inventory, security, and usage data to facilitate vendor/supplier third-party cybersecurity risk monitoring and reporting. Cylera also alerts when medical device manufacturers release security bulletins that impact assets in the asset inventory. |
| Enhanced CPGs                                                                         |                                                                                                                                                                                                                                                           |
| Asset Inventory                                                                       | Using patented Network Traffic Emulation™ and Adaptive Data Type Analysis™ technology, the Cylera platform provides unmatched device discovery and context for all healthcare IoT and connected medical devices across the entire healthcare network.                                                                                        |
| Third Party Vulnerability Disclosure                                                  | The Cylera platform provides robust vulnerability disclosure capabilities by correlating inventory against CVEs, misconfigurations, findings from the Cylera threat intelligence team, and information from medical device manufacturers, then provides prescriptive remediation guidance so response teams can act quickly.                 |
| Third Party Incident Reporting                                                        | The Cylera platform provides robust incident identification capabilities and detailed remediation guidance for threats specific to healthcare devices across vendors, enabling response teams to remediate incidents swiftly.                                                                                                                |
| Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures (TTPs) | The Cylera platform provides deep threat context by utilizing artificial intelligence (AI) and machine learning (ML) to correlate vulnerabilities, indicators of compromise (IOC), network behavior, and in-service data to reduce alert noise and allow users to quickly pinpoint and respond to actual healthcare IoT threats.             |
| Network Segmentation                                                                  | The Cylera platforms analyzes device behavior, then uses integrations with firewall and network access control (NAC) solutions to help enable the generation of network segmentation policies for healthcare IoT and connected medical devices.                                                                                              |
| Configuration Management                                                              | The Cylera platform automatically builds baseline network configuration policies for devices based on the type of device as well as device groups, which can then be used to ensure devices on the network adhere to appropriate device configuration standards.                                                                             |

Cylera provides the easiest, most accurate and extensible platform for healthcare IoT intelligence and security to optimize patient care, service availability, and cyber defenses across diverse connected medical device and healthcare environments. The Cylera platform accurately discovers, categorizes, assesses, and monitors known and unknown assets with high fidelity to deliver unparalleled asset inventory, usage telemetry, risk prioritization, analytics, and guided threat remediation. Cylera integrates with popular IT and healthcare systems to allow organizations to advance cyber program maturity, increase operational efficiency, mitigate cyber threats, and enable compliance readiness.



[www.cylera.com](http://www.cylera.com)