



## WHITE PAPER

# UNDERSTANDING HHS SECTION 405(d) & MEDICAL DEVICE SECURITY

## Medigate by Claroty and Health Industry Cybersecurity Practices (HICP) Technical Volume 2

When the Cybersecurity Act (CSA) became law in 2015, the landscape and frequency of cybersecurity threats to healthcare organizations looked very different than it does today. The traditional approach to cybersecurity in the healthcare space has revolved around the data privacy and security risks considerations of HIPAA. The Department of Health and Human Services (HHS) has released guidance, Cybersecurity Framework Implementation Guide, in an effort to move the Healthcare Industry away from focusing on HIPAA requirements to manage cybersecurity and transition to a risk based framework for a systematic approach to risk reduction. According to the Department of Health and Human Services:

*“The 405(d) Program aims to develop consensus-based best practices, and methodologies to strengthen the healthcare & public health (HPH) sector’s cybersecurity posture against cyber threats. After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group developed Health Industry Cybersecurity Practice: Managing Threat and Protecting Patients, its first official task group product.”*

In the Spring of 2023 Section 405(d): Aligning Health Care Industry Security Approaches was updated to include a deeper set of considerations around medical device cybersecurity in addition to the existing focus on consensus-based and industry-led guidelines, best practices, methodologies, procedures, and processes that serve to reduce cybersecurity risk to healthcare environments. Basing an organization’s cybersecurity program on an industry-recognized cybersecurity framework can also help direct capital, operational, and resource allocations to lines of business generating the greatest return on protecting assets/information and minimizing risk exposure.

Section 405(d) presents 10 practices, tailored to healthcare delivery organizations of all sizes, to help mitigate these threats. This document focuses on one of those ten practices: Cybersecurity Practice #9: Network Connected Medical Devices.

## Cybersecurity Practice #9: Network Connected Medical Devices

Healthcare delivery organizations use many diagnostic and therapeutic devices for patient treatment as well as building management systems (BMS) that control the healthcare environment itself, such as HVAC systems, connected thermostats, and elevator controls. These devices range from straightforward monitors that provide crucial information for healthcare providers to complex, multi-function machines that provide critical life-supporting care such as infusion pumps or respirators. Medical and BMS have similar cybersecurity deficiencies, create massive amounts of data that affect patient safety, well-being, and privacy, and their interconnection with traditional IT systems broadens the attack surface of healthcare networks.

The following sections outline Claroty's ability to support **Practice #9: Network Connected Medical Devices** and the associated sub-practice guidelines for **Medium (9.M.X)** and **Large (9.L.X) Healthcare Organizations**:

<b>9.M.A - Asset Management</b>	<b>3</b>
<b>9.M.B - Endpoint Protections</b>	<b>5</b>
<b>9.M.C - Identity and Access Management</b>	<b>6</b>
<b>9.M.D - Network Management</b>	<b>8</b>
<b>9.M.E - Vulnerability Management</b>	<b>10</b>
<b>9.M.F - Contacting the FDA</b>	<b>11</b>
<b>9.L.A - Security Operations and Incident Response</b>	<b>12</b>
<b>9.L.B - Procurement and Security Evaluations</b>	<b>14</b>
<b>Medical Device Security with the Medigate Platform</b>	<b>15</b>



9.M.A - Asset Management

NIST Framework Ref: ID.AM, ID.AM-1, PR.IP-6

Recommended Actions	What does this mean?
<p>As much as feasible, medical devices should have the following controls enabled:</p> <ul style="list-style-type: none"><li>• <b>Inventory, hardware:</b> All medical devices should be added to an inventory that is capable of reflecting the core components of the devices themselves. You may have to employ specialized tools designed specifically for tracking the lifecycle of medical devices. Such systems can be useful for maintaining preventative maintenance schedules.</li><li>• <b>Inventory, software:</b> Implement a software component inventory for your medical devices. Manufacturers should be able to deliver to the HDO a full listing of software components with at least major version information. Such lists are sometimes referred to as a software bill of materials (SBOM). Information about software components should be maintained in a scalable database managed by the HDO</li><li>• <b>Wiping:</b> When a medical device is slated for decommissioning, it is critical to ensure that all data on the device are wiped. Typically, these devices are returned to the vendor and potentially resold or delivered to other organizations for destruction. Federal and state requirements for the protection and disposal of hardware and media that maintain PII prohibit the allowing the data to be accessed by these other parties.</li></ul>	<p>Knowing what devices are on the network, how many there are, what they are connected to, and how they're communicating is the foundation of all other measures used to protect the network.</p> <p>This is no different for specialized systems like medical devices. However, this level of visibility can be difficult to achieve due to the unique ways in which medical devices communicate, as well as the device, infrastructure, and workflow complexities of healthcare environments.</p> <p>Without the ability to capture and ingest these protocols, medical devices are invisible to security tools and therefore left vulnerable to risks.</p>

How Claroty Supports 9.M.A - Asset Management

Claroty's Medigate platform enables HDOs to implement all controls recommended by 9.M.A. Specifically, the platform automatically discovers all medical devices in a customer's environment, creates a central inventory for this information — including all core hardware and software components and related details for each device — and continuously updates such information to keep the inventory up-to-date.

Medigate's asset management capabilities are highly differentiated for two key reasons. First, the platform supports the broadest and deepest library of medical device and IoT protocols in the industry, ensuring visibility even into devices that utilize among the most obscure — and otherwise impossible to decipher — proprietary protocols. Second, the platform gives customers the option to easily combine two different device discovery methods to suit their needs.




Unlike status-quo solutions — which only offer one method, passive monitoring, for device discovery — Medigate is purpose-built to address the reality that while many devices can be discovered using a passive-only solution, the complex nature of modern healthcare environments often requires more. This is why the Medigate Platform employs the following two, highly flexible discovery methods:

- **Passive Monitoring:** PPassive monitoring provides a complete profile of observed assets, including dozens of attributes that go beyond IP/MAC identification, such as model number, firmware version, OS, and more, and is considered a best practice by the Health Sector Coordinating Council (HSCC). Claroty correlates this information with known vulnerabilities and risks, and maps communication patterns that can be used to create policies or show signs of potentially erroneous or malicious behavior.
- **Claroty Edge:** A first-of-its-kind solution that delivers comprehensive visibility into hard-to-reach areas in healthcare networks in minutes without requiring network changes or sensors.

Device Information

Risk & AlertsManufacturer InfoLocationNetwork ConnectivityNetwork SecurityUtilizationHistory



#ID: BAFTEIB

8100 Pump Module

Alaris

RISK SCORE: VERY LOW (21.2)

+ Add Note

LABELS

1-25Label1

+ Add Assignees

1 MDS\* File

+ Upload MDS\* Files

DEVICE INFORMATION

Device IDs	IP	10.13.15.214 / 1210287664	MAC	00:10:7A:CE:00:12	MAC OUI	Ambicom (was Tandy?)	CATEGORY	Medical	SUB CATEGORY	Patient Devices
	MANUFACTURER	Alaris	TYPE	Infusion Pump Module	MODEL	8100 Pump Module	MOBILITY	Portable	SERIAL NUMBER	1210287664
	FDA CLASS	2								
Versions & Names	OS	Proprietary Micro Digital SMX R...	OS NAME	Proprietary	OS VERSION	Micro Digital SMX RTOS	SW / FW VERSION	9.17.0.22		
Network	NETWORK	Corporate	NETWORK SCOPE	Default	VLAN	902	VLAN NAME	WIFI_902	VLAN DESCRIPTION	WIFI_902
	CONNECTION TYPE	Gateway	IP ASSIGNMENT	Static	WIRELESS ENCRYPTION	WPA2	FIRST SEEN	1/12/23, 8:53 AM	LAST SEEN	3/23/23, 4:37 PM
Location	SITE NAME	Albany	LOCATION (PROTOCOL)	Adult	AP BSSID	00:C0:58:50:43:E0	SSID	MEDNET	AP NAME	BR03030014
	AP LOCATION	bronx > Building 4 > Floor 4	LAST SEEN ON AP	3/23/23, 5:05 PM	COLLECTION INTERFACES	ens142@demo-collection-bronx...				
CMMS & CMDB	CMMS ASSET TAG	CL110215656	CMMS MANUFACTURER	Alaris	CMMS MODEL	8100 Pump Module	CMMS STATE	In Service	CMMS OWNERSHIP	Rental
	CMMS DEPARTMENT	Recovery Room	CMMS BUILDING	Diagnostic Center	CMMS FLOOR	2	CMMS ROOM	Room 11	CMMS LAST PM DATE	2/8/23, 3:49 PM
	CMMS COST CENTER	Cardiac Diagnostic	CMMS FINANCIAL COST	6821\$						
Users & Apps	MDM LAST SYNCED	3/23/23, 4:36 PM								

Fully enriched device details of an individual medical device within the Medigate Platform

Using the above discovery methods, the Medigate Platform is able to uncover each device’s IP, MAC address, vendor, model number, firmware version, and additional details. The platform then automatically assesses and enriches this information to provide a comprehensive profile for each device complete with inherent risk and vulnerabilities, communication patterns and recommended network policies, and lifecycle information for utilization and planning.

When it comes to devices that are slated for decommissioning, the Medigate Platform provides a simple way to identify which devices on the network store PHI so that they can be routed to the proper workflows for decommissioning.

© 2023 Claroty Ltd. All rights reserved

4

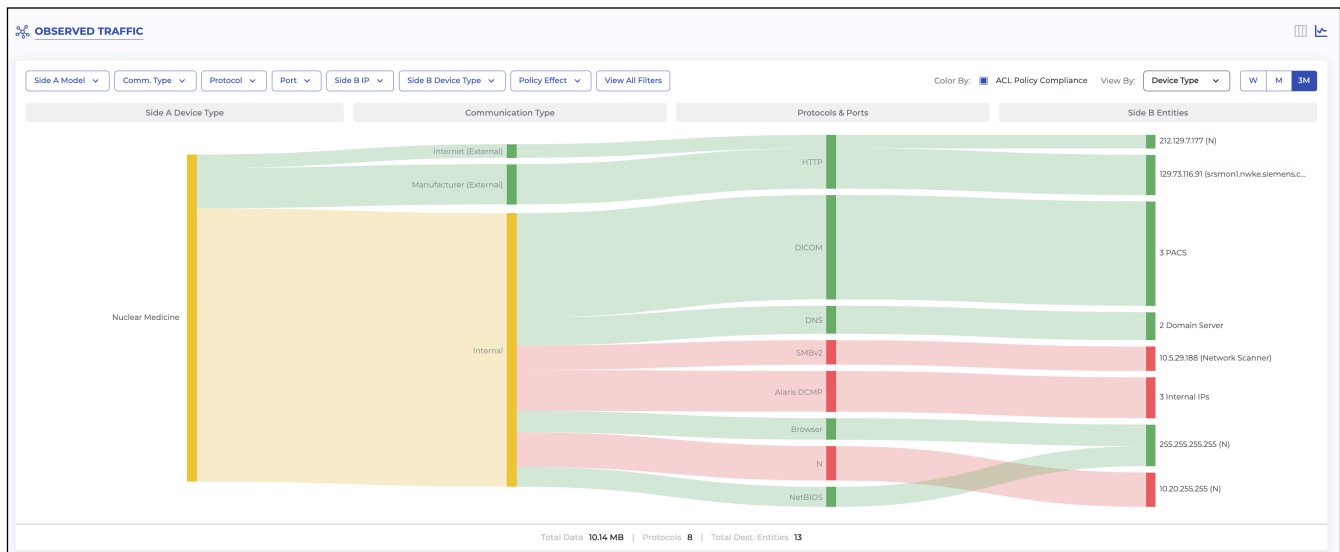
9.M.B - Endpoint Protections

NIST Framework Ref: PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1

Recommended Actions	What does this mean?
<p>Where feasible, medical devices should have the following controls enabled:</p> <ul style="list-style-type: none"><li>• <b>Antivirus software:</b> Usually, the medical device manufacturer should directly support AV software, or it should be cleared for operation by the manufacturer. Ensure that a compliant AV technology is enabled. If AV cannot be implemented, compensating controls should enforce an AV scan whenever the device is serviced prior to reconnecting to the device network.</li><li>• <b>Local firewalls:</b> Medical devices should be configured to communicate only with other required systems. Unused services and ports should be disabled if supported by the manufacturer.</li><li>• <b>Encryption:</b> Data stored on the device should be encrypted in the event of a device being misplaced</li><li>• <b>Application whitelist:</b> Configure medical devices to only allow known processes and executables to run on the devices. This control alone can significantly reduce the exploitability of devices.</li><li>• <b>Default password changes:</b> If supported, medical devices should require default password changes</li><li>• <b>Routine patching:</b> Medical devices should be monitored and updated as relevant updates are released by manufacturers as part of preventative maintenance cycles. This control, along with whitelisting, can significantly reduce the exploitability of the device</li></ul>	<p>The endpoint protection controls recommended by 9.M.B both reinforce the importance of securing medical devices and validate that such devices cannot always be secured by standard solutions or approaches to endpoint protection.</p> <p>Specifically, most endpoint protection solutions — such as antivirus and EDR software — take an agent-based approach that assumes software can be installed and continuously run on a device. Standard approaches also assume that software patches can be routinely applied to a device.</p> <p>However, while those types of standard controls are suitable for standard information technology (IT) devices such as laptops, they are not always suitable for medical devices. Here’s why:</p> <ul style="list-style-type: none"><li>• Medical devices underpin care-delivery — and often, a patient’s health and safety relies on a device to operate continuously. Since software patches generally cannot be applied while a device is operational, frequent patching may not always be possible.</li><li>• Many medical devices use legacy operating systems (OS) that are not simply supported by endpoint protection solutions.</li><li>• Many medical devices — regardless of their OS — cannot tolerate the added processing resources consumed by agent-based solutions without the risk of compromising a device’s ability to operate and safely support the care-delivery operations it is intended to support.</li></ul> <p>In light of the above limitations, HDOs are encouraged to implement layered security control — including those recommended by 9.M.B — to restrict access to devices at various levels within the network to ensure they remain operational and/or prevent the further spread of an incident.</p>

How Claroty Supports 9.M.B - Endpoint Protections

Claroty’s Medigate Platform offers extensive native and integrated capabilities that support the endpoint protection controls recommended by 9.M.B. Specifically, the superior visibility the platform provides into all devices on the network enables it to reveal which devices are compatible with agent-based endpoint protection solutions — most of which Medigate also integrates with seamlessly. Such integrations enable users to then extend their existing solutions’ agent-based protections to the unmanaged devices for which doing so is safe.



Device communication and policy adherence flow within the Medigate Platform

Furthermore, for all devices — regardless of whether they can or cannot tolerate agents — Medigate harnesses its visibility into device communications to automatically define policies that can be enforced by a customer’s firewalls and/or network access control (NAC) solutions to segment the network. This capability supports 9.M.B’s recommendation to configure devices to communicate solely with required systems, as well as to deploy compensating controls to mitigate the risks facing agent-intolerant and/or unpatchable devices.

In terms of patching, the Medigate platform supports this control by automatically and continuously correlating all devices on the network against the latest common vulnerabilities and exposures (CVEs) and other security weaknesses from the industry’s largest database of vulnerabilities from both open and proprietary sources. Each device is also assigned a customizable risk score based on its unique characteristics — including the presence of any unpatched vulnerabilities, its location and connections within the network, whether it stores PHI, and more — and the unique risk posed to the network. As a result, customers can more easily identify, prioritize, and remediate and/or compensate for vulnerabilities based on risk.

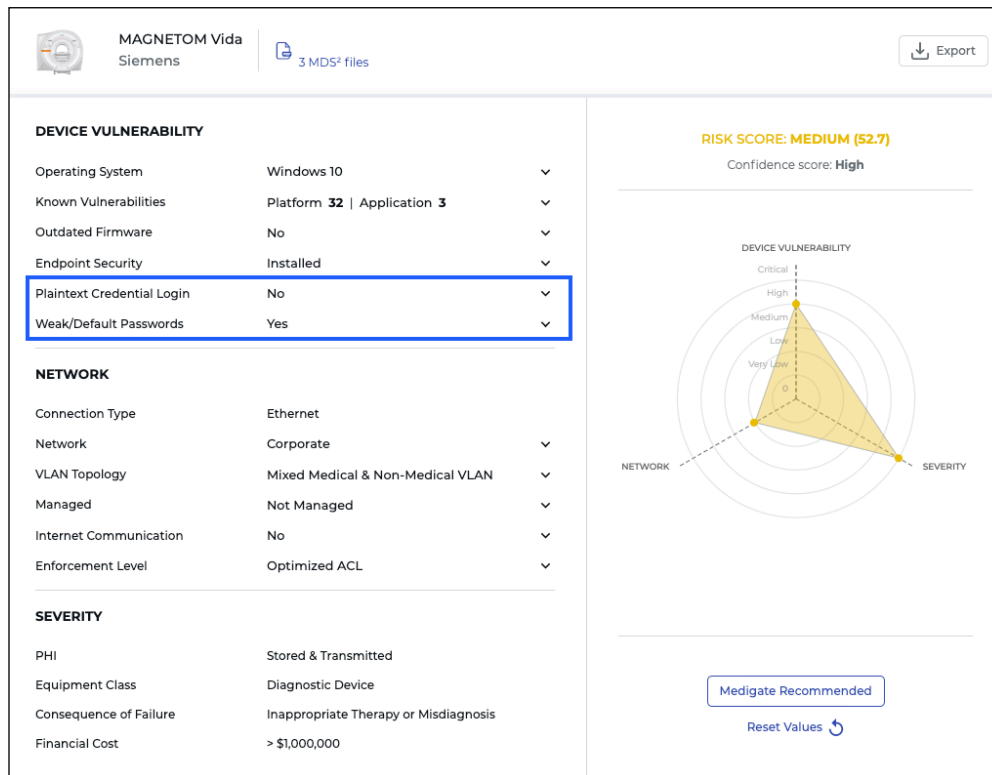
## 9.M.C - Identity and Access Management

NIST Framework Ref: PR.AC, PR.AC-7, PR.AC-4

Recommended Actions	What does this mean?
As much as feasible, medical devices should enable <b>strong authentication, complex passwords, and secure remote access</b> . The foundation of identity and access management (IAM) solutions is to ensure accurate detection and tracking of every asset and user that connects to the network. In a similar challenge to previous practices, many mature solutions for IAM use agents to manage access to devices. Getting around this challenge requires solutions to provide an accurate fingerprint of every device that connects to the network including in-depth details of its hardware, software, security risks, and communication patterns.	Because medical devices can be difficult or impossible to manage via agents, device communication patterns are often the most reliable way to monitor for malicious activities caused by unauthorized access. Understanding what “normal” network behavior looks like for specific devices, as well as their context within healthcare delivery workflows will provide the foundation required to mitigate potential threats that are able to circumvent access controls.

## How Claroty Supports 9.M.C - Identity and Access Management

HDOs can use information from the Medigate Platform to enrich all controls mentioned in 9.M.C - Identity and Access Management. In addition to the communication profiling and monitoring covered in 9.M.D - Network Management, the Medigate Platform integrates with a number of the leading security and asset management solutions to enrich identification for devices protected by these solutions including OS details, Installed apps and more. This, among other attributes such as the use of plaintext credentials and weak/default password usage, build into a comprehensive risk score for every device on the network. The effect of risk factors like these can be simulated to help drive remediation actions based on calculated impact to ensure the most effective and efficient use of risk reduction efforts.



*Device risk simulation for a critical medical device showing noted IAM controls from 9.M.C - Identity and Access Management*

In addition to these integrations, the Medigate Platform offers its own robust role-based access controls (RBAC) that allows administrators to provide granular access to users based on role and access needs. This means that user views can be completely customized to their required access and workflows, providing only the information they need, both enhancing the security of the Medigate Platform and creating a simple, intuitive interface for the user.

9.M.D - Network Management

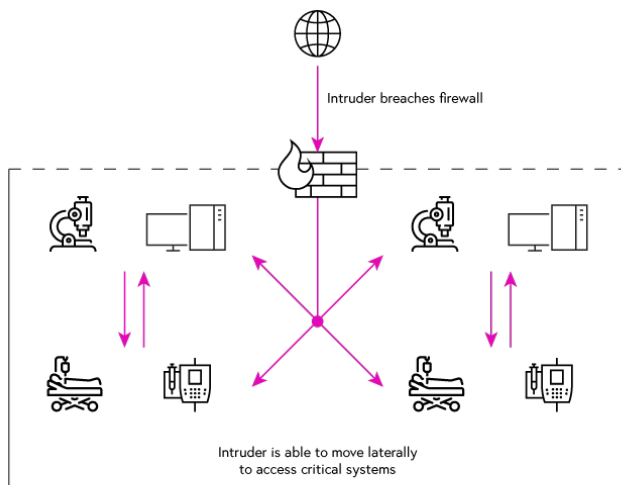
NIST Framework Ref: PR.AC-5

Recommended Actions	What does this mean?
<p>As much as feasible, medical devices should have the following controls enabled:</p> <ul style="list-style-type: none"><li>• <b>Segmentation:</b> Given the critical nature of medical devices and the organization’s general inability to configure them to reduce vulnerabilities. The ability to restrict access to the device is essential to its safe operation—only traffic which is required for operation should be allowed on these networks. Access to device management systems should be heavily restricted to limit its exposure.</li><li>• <b>Microsegmentation:</b> Takes segmentation one step further by protecting devices from other systems in the same network segment in addition to systems outside of their network. It is based on the concept of Zero Trust and is the most effective way to protect devices.</li></ul>	<p>Network segmentation is critical to helping ensure safe and uninterrupted care delivery. Achieving this requires the creation of policies that allow network traffic based only on the required operational needs of devices. Additionally, communication access to medical devices should be based on the <b>principles of Zero Trust</b>, the core of which being that no person or device should have unrestricted access to other devices.</p> <p>Medical devices are purpose-built for specific communication patterns and methods, making them well-suited for this level of segmentation. However, this approach can be challenging for two reasons:</p> <ul style="list-style-type: none"><li>• <b>Cost prohibitive:</b> Without an automated solution, this level of segmentation requires clinical engineers to map device communications and program barriers to enforce communication policies.</li><li>• <b>Difficult to implement:</b> Clinical workflows mean that devices often move around a hospital setting freely, segmentation policies must take this into account when restricting access and communication across subnets.</li></ul> <p>In this regard, clinical workflows often contradict standard IT cybersecurity procedures. It is especially important to highlight that <b>these practices must be put into place within a clinical context</b> to avoid disruption to patient care delivery.</p>

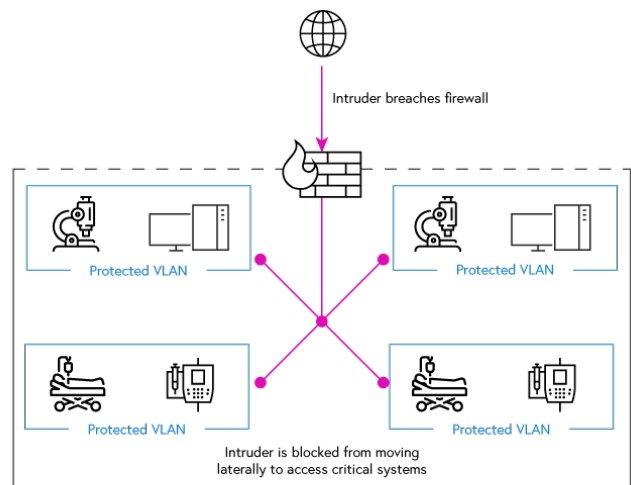
How Claroty Supports 9.M.D - Network Management

As a major control in the journey towards achieving cyber resilience and protecting healthcare delivery, the Medigate Platform supports all aspects of 9.M.D - Network Segmentation. Distinguishing legitimate communication across business processes and applications requires an accurate and detailed inventory of devices including how and why devices are communicating. Frequently, ineffective or completely nonexistent segmentation between devices is the root cause of many aspects of network risk.





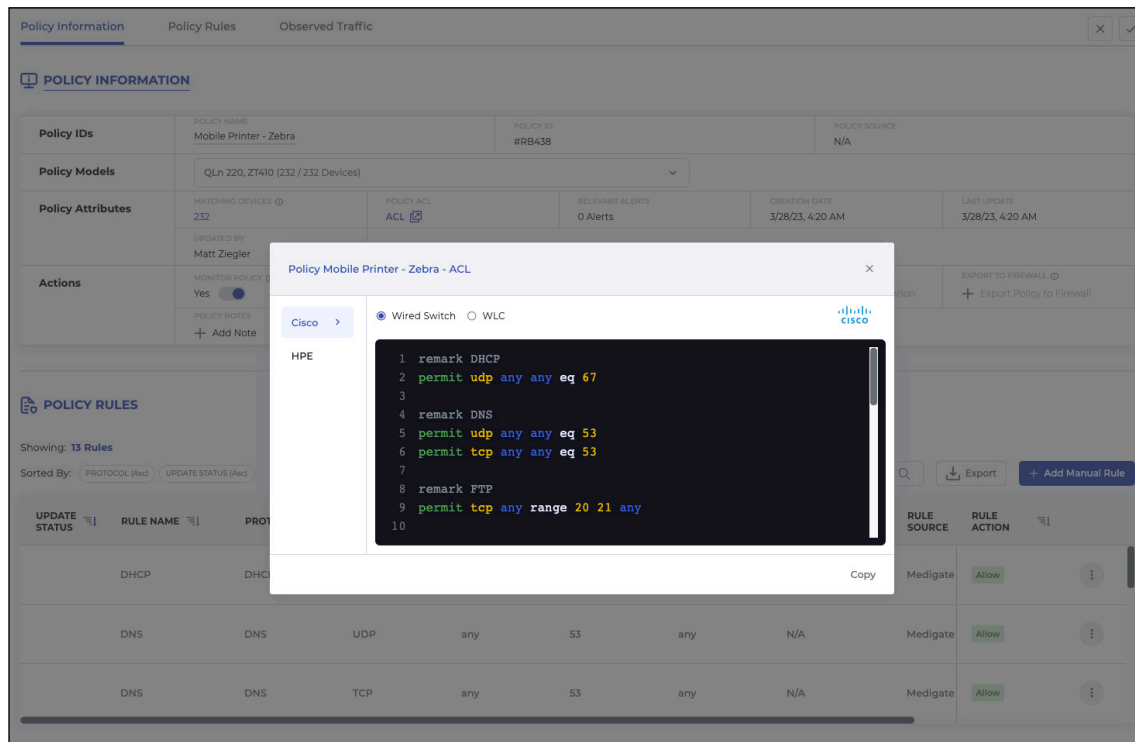
**Without Network Segmentation**



**With Network Segmentation**

*A look with and without network segmentation within a clinical environment*

The Medigate Platform profiles all device communication on the network in order to understand how and with what each device communicates. This sets a foundation for what “normal” network behavior looks like. With these device communication profiles, the Medigate Platform automatically creates recommended communication policies based on network context and industry best practices. These communication policies can be customized, monitored for a period of time to ensure stability, and automatically pushed to third party tools such as NAC and Firewall solutions.



*Automated ACL generation based on recommended communication policies with the Network Security Management module of the Medigate Platform*

These policies effectively segment the network into subnets of devices that are known to communicate under normal circumstances, or communicate according to industry best-practices, automatically—therefore eliminating the costly and time consuming task of manual segmentation. These capabilities support clinically contextualized Zero Trust programs that help protect clinical workflows as much as they protect devices.

9.M.E - Vulnerability Management

NIST Framework Ref: ID.RA-1, PR.IP-12, ID.RA-5, RS.CO-5, DE.CM-8

Recommended Actions	What does this mean?
<p>As much as feasible, medical devices should have the following controls enabled:</p> <ul style="list-style-type: none"><li>• Vulnerability and risk categorization: according to the 2016 Postmarket Management of Cybersecurity in Medical Devices guidance issued by the FDA, medical device manufacturers and HDOs should implement vulnerability and risk-management practices to categorize risks according to the device’s effectiveness and the potential to cause harm to the patient. Utilizing a risk-based approach to vulnerability management permits flexibility that can address the problem of scarce resources on tasks that mitigate and reduce risk to the organization. Asset Discovery &amp; Security and computerized maintenance management systems (CMMS) tools can be imported and correlated against the HDO’s inventory to automatically alert on devices with vulnerabilities/exploits, recalls, or other known risks.</li><li>• As mentioned in Sub-Practice 9.M.A - Asset Management, medical devices often ship with an SBOM. Using SBOMs the HDO can compare the organization’s software libraries with known vulnerabilities. This comparison provides the HDO with information on current potential vulnerability postures in the medical device space.</li><li>• Vulnerability scanning: The final action that an HDO can take to understand its vulnerability posture is to conduct vulnerability scans against the medical devices. <b>The device should be in a highly controlled setting and not connected to a patient when performing these scans.</b> A vulnerability scan can be configured to profile the device and determine whether potential vulnerabilities exist, or to confirm that vulnerabilities have been mitigated as part of a remediation or patching plan.</li></ul> <p>Sub-Practice 9.M.E also contains information detailing best practices within contract negotiating to ensure that cybersecurity considerations are included in this process.</p>	<p>No network is without risk and the complex architecture of a modern healthcare delivery organization makes understanding risk a challenging endeavor. In order to more effectively and efficiently reduce risk hospitals must understand how the intersection of device, infrastructure, and workflow complexities create it.</p> <ul style="list-style-type: none"><li>• <b>Device Risk:</b> Involves the inherent risks and vulnerabilities that exist within connected devices such as known CVEs, misconfigurations, manufacturer end-of-life indicators, external communications, and more.</li><li>• <b>Infrastructure Risk:</b> Devices are typically on the same network meaning that every new device added introduces a new level of risk, exposing care delivery and PHI to external networks.</li><li>• <b>Workflow Risk:</b> Care delivery workflows are often incompatible with standard IT cybersecurity practices. This requires the addition of clinical context to security protocols which are often decentralized and lack ownership in healthcare environments.</li></ul> <p>Due to the nature of these environments, traditional methods for identifying and addressing vulnerabilities are not always suitable for HDOs. An example of this is the reference in 9.M.E to using scanning as a method of vulnerability identification. While these solutions can be effective at identifying risk, the delicate nature of IoMT devices means that improper scanning could result in a medical device being rendered unusable and could potentially impact patient care.</p> <p>Examples like this are why a clinical context is imperative to proper vulnerability management in healthcare environments.</p>

## How Claroty Supports 9.M.E - Vulnerability Management

The ability to resolve network risk in the most effective and efficient way is the core of the Medigate Platform's support for 9.M.E - Vulnerability Management. As stated above, no network is immune to risk, but knowing which actions will have the greatest impact on reducing risk in the environment is critical to maintaining a strong cybersecurity posture.

The Medigate Platform enables users to customize network's risk configuration profile, resulting in a tailored network risk score and curated recommendations for network-wide risk reduction actions. In order to provide the most accurate assessment vulnerabilities in the network, Claroty works with leading medical device manufacturers (MDM) and pulls information from the CISA Catalog of Known Exploited Vulnerabilities (KEV) in order to pinpoint exactly which vulnerabilities are present and known-to-be-exploited within the devices in the network.

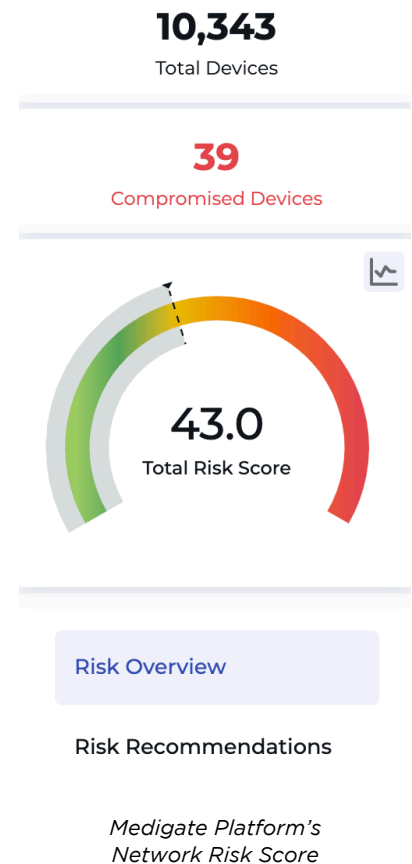
By correlating network and asset details with our vulnerability and risk knowledge base, Claroty uncovers risk blindspots that take the form of unpatched CVEs, misconfigurations, poor security practices, and unsecured protocol usage to:

- **Provide Multi-Factor Risk Scores** that reveal the true risk of an asset as it relates to an organization's unique environment
- **Enable and Measure Comprehensive Risk Reduction** by helping organizations prioritize remediation of vulnerabilities most likely to be exploited

Because healthcare networks contain a variety of device types, the Medigate Platform integrates with leading industry vulnerability scanners that enable hospitals to safely orchestrate and deploy targeted vulnerability scans to uncover IT device risk within healthcare networks. This is possible through the Medigate Platform's ability to include or exclude scannable devices by identified device attributes to ensure that critical devices are not erroneously scanned and negatively impacted. The result is a complete picture of network risk across all device types, contextualized within specific network profile, with the ability to streamline vulnerability management workflows and remediation efforts.

### 9.M.F - Contacting the FDA

NIST Framework Ref: RS.AN-5



Recommended Actions	What does this mean?
According to Section 405(d) Volume 2, if a HDO discovers or is notified of a high-risk cybersecurity vulnerability and cannot receive support from the medical device manufacturer to mitigate this risk, the HDO's has recourse to contact the FDA directly to file a complaint concerning the vulnerability. Contacts to the FDA should be limited to critical or high-risk scenarios, especially those with the potential to cause harm to patients.	As the oversight organization for the majority of medical devices found in healthcare environments, the FDA is a key stakeholder in building a strong foundation of healthcare cybersecurity practices.

## How Claroty Supports 9.M.F - Contacting the FDA

All of the data captured, analyzed, and curated by the Medigate Platform can be distilled into highly customizable, dynamic, and automated reports. Types of data shown in these reports can include network device management data, top risk sources and trends over time, network communication and policy overviews, and more. These reports can also be saved into templates and run and sent to specific users or groups, automatically, at a predefined interval.

### 9.L.A - Security Operations and Incident Response

NIST Framework Ref: PR.IP-9, DE.CM-8, DE.CM-1, DE.CM-7

Recommended Actions	What does this mean?
<p>HDOs can provide monitoring, detection, and response activities around their medical device ecosystems using many processes already existing in their IT device workflow. Using methods like segmentation outlined above, HDOs should monitor for malicious activity across the network and integrate network and device data into solutions like log management systems and SIEMs.</p> <ul style="list-style-type: none"><li>• HDO's should strive to consolidate all device information into a cloud-based CMMS. By replacing multiple maintenance management systems and databases containing disparate data elements into one CMMS, an HDO can position itself for a single device inventory that is integrated with ADS solutions to orchestrate the remediation of cybersecurity events. This includes preventative maintenance, corrective maintenance, contract, cost of ownership, capital planning and asset discovery and security data and events. Just as the Clinical Engineering team responds to preventative maintenance work orders in the CMMS system, HTM and Network Engineers can respond to a CMMS' security maintenance work orders. Coordinated remediation processes via workflow management provides security context and impact of the event, including what patch, configuration change, or mitigating controls are required to then determine the remediation priority.</li><li>• Device baselines are the learned and/or monitored communication patterns for a device. Once an HDO has identified all of its connected medical devices, determining their purpose in the network and understanding its normal behavior patterns is an essential to medical device cybersecurity. Baselines are essential to an HDOs ability to detect and respond to anomalous device behavior.</li></ul>	<p>Putting this information into a clinical context is another critical step in a maturing security operations and incident response program. Does the device transfer or store ePHI? Which connections are clinical and which are non-clinical? Without manual intervention this information can be difficult to verify for medical devices using traditional IT security tools.</p> <p>To increase cohesion across network tools and to provide visibility into the daily operations of the medical device systems in relation to the broader IT network, medical device information sources should be integrated with existing tools such as the HDO's CMDB, SIEM, firewall, intrusion prevention system, log management systems, and more.</p> <p>As mentioned within the sub-practice description, integrating existing solutions into a single-source of truth will drive opportunities to create more effective, efficient, and secure care delivery workflows and medical device management practices.</p>

## How Clarity Supports 9.L.A - Security Operations and Incident Response

The Medigate Platform's unified insights and alert system provides automated methods to monitor, prioritize, and respond to affected devices through an unmatched depth of device visibility and remediation workflow capabilities. This system is the root of our support for Sub-Practice 9.L.A - Security Operations and Incident Response. Network information can be integrated with a number of existing tools such as SIEM, SOAR, CMDB, and Firewalls in order to enhance the coverage and return-on-investment (ROI) of these solutions.

Building on the foundation of complete and accurate visibility and device communication mapping the Medigate Platform provides vulnerability and anomalous communication alerts. Inter-device communication relationships can be narrowed down in a list to specific affected devices or visualized on a world map, within a connection matrix, and a communication flow diagram in order to better understand network traffic and potential areas for risk. The categories of insights and alerts within the Medigate Platform are:

- Communication: Generated based on inbound/outbound external communications
- Device: Based on discovered device data such as known vulnerabilities
- Segmentation: Alerts that are based on VLAN rules
- Policy Deviation: Generated by network asset rules for outbound traffic
- Custom: Alerts created for specific network conditions defined by administrators

[Alert Information](#) [Affected Devices](#) [Events](#) [History](#)

### Attempted Malicious Internet Communication (Alert #1000013)

[Resolve All](#) [Acknowledge](#)

Attempted outbound Internet communication detected between reported malicious IP address 212.129.7.177 and 8 devices

ALERT INFORMATION

ALERT STATUS <b>Unresolved</b>	ALERT CATEGORY <b>Threat</b>	AFFECTED SITES 2 Sites	DETECTED 11/21/22, 11:45 AM
UPDATED 11/21/22, 11:45 AM	IP 212.129.7.177 <a href="#">Mark as Not Malicious</a>	DOMAIN a.gowin7.com	GEO LOCATION France
+ Add Notes		+ Add Labels	ASSIGNEES <a href="#">Ash Marshick</a> <a href="#">Steve Janke</a>

Powered by **ANOMALI**

SEVERITY <b>High</b>	CONFIDENCE <div><div></div>100%</div>	THREAT TYPE Malware	SOURCE droplist_high_confidence OSINT
LAST UPDATE 6/18/22, 1:37 PM	IP TYPE Malware C&C IP	TAGS <a href="#">stdominics.edu:droplist</a>	

**Recommendations**

Block or monitor traffic to/from the malicious IP that is flagged by this alert. This is best addressed at the perimeter FW.

*Communication alert due to a malicious communication attempt generated within the Medigate Platform*



9.L.B - Procurement and Security Evaluations

NIST Framework Ref: ID.SC

Recommended Actions	What does this mean?
<p>HDOs should establish a set of cybersecurity requirements during the acquisition of medical devices. These requirements should be memorialized in the organization’s contracting processes and implemented through the supply chain and procurement functions. Cybersecurity requirements should be incorporated into prospective procurements through vendor requests for information (RFIs) or requests for proposals (RFPs). Security considerations in medical device security procurement are:</p> <ul style="list-style-type: none"><li>• <b>Security evaluations:</b> HDOs should consider requiring a Manufacturer Disclosure Statement for Medical Device Security (MDS2) for all eligible devices. These provide a list of comprehensive cybersecurity questions for medical devices with manufacturer responses</li><li>• <b>Contract negotiation:</b> Cybersecurity personnel should review and provide input into the contract with the manufacturer and should highlight security requirements. These requirements should reference the FDA’s Postmarket Management of Cybersecurity for Medical Devices guidance.</li><li>• <b>SBOM:</b> The HDO should request an SBOM as part of the procurement process. Understanding the software libraries that make up the device enables the HDO to understand the potential risk of the device.</li><li>• <b>End-of-life and support:</b> Manufacturers should disclose device life expectancy in order to help HDOs asset management plan. This plan should include expectations for when end of life (EoL) and end of support (EoS) will occur.</li></ul>	<p>Planning for and maintaining a foundation for a strong security posture begins before a device even enters the network. Understanding what risk looks like within a healthcare environment is essential to ensuring that proper measures are taken before new devices are onboarded.</p> <p>MDS2 forms are a key part of this process. An MDS2 is an industry standard format developed by the Health Information Management and Systems Society and the American College of Clinical Engineering that has been adopted by most medical device manufacturers. It provides a list of comprehensive cybersecurity questions for medical devices, with responses from the manufacturer of the device in question.</p> <p>This form can be used as a guide for procurement and contract negotiations, highlighting key strengths and weaknesses of medical devices as it relates to their security. Going beyond the MDS2, it is essential to maintain the ability to monitor a device throughout its entire lifecycle by understanding when a device will reach its end-of-life status, in other words, when it no longer receives software updates from the manufacturer. This information can be used for procurement planning, but also for implementing compensating controls like those covered in 9.M.D - Network Management.</p> <p><i>For more information on Medical Device Contract Language see the HSCC publication of pre-negotiated contract language created by MDMs and HDO; <a href="#">Model Contract Language for MedTech Cybersecurity (MC2)</a></i></p>

How Claroty Supports 9.L.B - Procurement and Security Evaluations

The Medigate Platform supports all aspects of 9.L.B - Procurement and Security Evaluations by providing HDOs with the information and capabilities required to evaluate and plan around the lifecycle of connected devices. The Medigate Platform hosts a comprehensive MDS2 database to help users drive better decision making from risk reduction planning to device procurement by matching existing network devices to known MDS2 forms with the ability to compare these forms by specific questions.

QUESTION NUMBER	QUESTION	PLUM 360 W/MEDNET ... ICU Medical, Inc. / Infusi...	BD ALARISTM PC UNIT,... BD / Infusion Pump	8015 CareFusion / Infusion Pu...
MPII-1 ⓘ	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information...	Yes	Yes, See Note ⓘ	Yes, See Note ⓘ
B.1 ⓘ	ePHI Data maintained by the device: Demographic (e.g., name, address, location, unique identification number)?	No	Yes, See Note ⓘ	Yes, See Note ⓘ
B.2 ⓘ	ePHI Data maintained by the device: Medical record (e.g., medical record #, account #, test or treatment date, device identification...	Yes	Yes, See Note ⓘ	Yes, See Note ⓘ
B.3 ⓘ	ePHI Data maintained by the device: Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying...	No	Yes, See Note ⓘ	Yes, See Note ⓘ
B.4 ⓘ	ePHI Data maintained by the device: Open, unstructured text entered by device user/operator?	No	Yes, See Note ⓘ	Yes, See Note ⓘ

MDS2 form comparison within the Medigate Platform

In addition to this, The Medigate Platform delivers insights such as device location, utilization, and inventory statistics, along with benchmarked and actionable recommendations. With this information HDOs can optimize inventories via lease/purchase quantities and right-size maintenance agreements. By pulling in information from existing device inventories and integrations, continuously monitoring device communications and usage, and bringing in industry benchmarks, Claroty helps transform an HDO's CMMS into a connected, dynamic, and data-rich system of record that can streamline and mature BioMed and IT workflows.

## Medical Device Security with the Medigate Platform

The Medigate Platform exists because delivering high-quality care in the age of connectivity requires resilience. This connectivity brings new challenges to an already complex environment surrounding devices, infrastructure, and clinical workflows.

Claroty offers the only solution to extend the full length of an HDO's cyber-physical security journey through core cyber and operational resilience controls. Whether its safe and compliant care delivery, operational efficiency, or cost optimization, it is the only platform that can meet users where they are regardless of the architecture, scale, or diversity of user base across core healthcare cybersecurity needs:

- Vulnerability & Risk Management
- Network Protection
- Threat Detection
- Device Management
- Lifecycle Management
- Operational Intelligence

To learn more, visit [www.claroty.com](https://www.claroty.com)

## About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit [claroty.com](https://claroty.com) or email [contact@claroty.com](mailto:contact@claroty.com).