

Improving Medical Device Security by Moving from Shared to Defined Responsibility

Authors:

Carsten Emmerling and Dr. Hans-Martin von Stockhausen, Siemens Healthineers
David Clark and Tom Pendergast, Roche Diagnostics
Phil Englert, Health-ISAC





Contents

- Scope Statement 1**
- Key Takeaways. 2**
- Introduction 3**
 - 1. Defining task responsibility among stakeholders reduces the overall risk of failure. 3
 - 2. Responsibility Assignment Matrix 5
 - 3. Responsibility distribution from software solution to cloud service 6
 - 4. Procedure to identify and describe defined responsibilities, set up a RACI matrix and a continuous improvement cycle 8
- Appendix 1 17**
 - MDM RACI example 17
- Definitions. 21**
 - Medical device 21
 - References 21



Scope Statement

Improving Medical Device Security by Moving from Shared to Defined Responsibility

Maintaining medical devices and systems requires the knowledge and skills of several different specialists. Those specialists may be provided by different organizations depending on the limitations in skills and capacities. This is especially true for the cybersecurity controls needed for regulated medical devices where traditional update, patch, and vulnerability management processes are complex. The concept of 'shared responsibility' distributes these tasks among different organizations. Historically, each group has made the assumption that some tasks such as vulnerability management, configuration, hardening, access control, etc., were to be completed by the other party, resulting in unaddressed vulnerabilities that would allow a hacker to exploit patient care technologies. Discussions with Healthcare Delivery Organizations (HDO) and Medical Device Manufacturers (MDM) have identified the need for a more defined approach to ensure that all responsibilities necessary to develop, implement, and operate medical devices are assigned to either the HDO or MDM. Identifying which security tasks each party is responsible for can improve the overall security posture of medical devices.

A responsibility assignment matrix is a commonly used methodology to define and manage the cooperative agreement between support entities and stakeholders. This white paper uses the Responsible/Accountable/Consulted/Informed (RACI) matrix as an example of a responsibility assignment matrix for purposes.

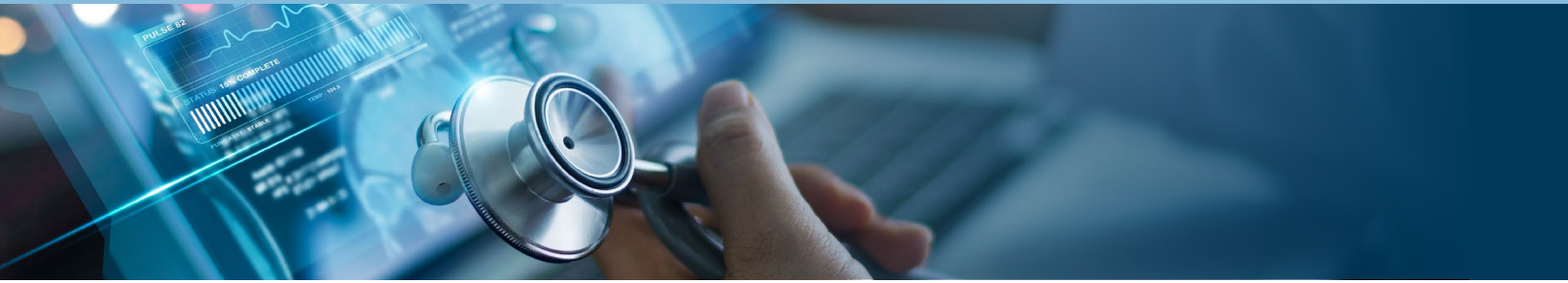
The paper presents a method to create individual RACI matrixes for common security deployment types for medical devices, based on templates defining standard deployment scenarios and a pool of tasks with suggested responsibilities. It includes two example matrices, MDM-managed and software-only devices.



Key Takeaways



1. Defining task responsibility among stakeholders reduces the overall risk of failure.
2. A responsibility assignment matrix helps to define task obligations for all parties supporting medical devices.
3. Gain an understanding of the responsibility distribution in operating software solutions through “black box” medical devices to cloud service.
4. Learn about procedures to identify necessary tasks and assign those tasks to responsible parties, set up a RACI matrix, and keep it updated with a continuous improvement cycle.
5. Find a RACI matrix template to define responsibilities for operational use.



Introduction

With the proclamation of October as National Cybersecurity Awareness Month, the Food and Drug Administration (FDA) is encouraging medical device manufacturers to brush up on their best practices and engage in good cyber hygiene. “As medical devices become more interconnected through wired and wireless connections, they also become more vulnerable, which could potentially impact patient safety,” according to an agency release. “At FDA, we strongly believe that medical device cyber safety is a large and shared responsibility that requires diligence from all stakeholders, including medical device manufacturers, government agencies, health care organizations, health care professionals, cybersecurity researchers, and medical device users.” The European Union (EU) Medical Device coordination Group (MDCG) described a joint responsibility scenario in **Guidance on Cybersecurity for Medical Devices¹** identifying participant roles and respective expectations. **Maturing to a clear definition of responsibilities for all cybersecurity maintenance activities is essential to improving resilience of the connected medical device ecosystem.**

1. Defining task responsibility among stakeholders reduces the overall risk of failure



Figure 1. Unclear responsibility assignment (Courtesy of Siemens Healthcare GmbH)



The term “shared responsibility” can help find common ground in discussions with multiple stakeholders. Medical device technologies are often complex and require multiple specialty skills to support. When a cybersecurity incident occurs, legal departments will try to pinpoint the actual responsible party to blame. In cases where the preventive activities may have helped to avoid the incident but were not defined upfront, discovering where the breakdown occurred is a challenging and complex process, even if the root cause, e.g., a “breach because of a missing patch,” is identified.

Common potential causes of cyber events may include:

- Patch was not provided or applied
- Threat actor in the network or with device access
- Incorrect configuration
- Employee negligence

Even in non-incident scenarios, the MDM and HDO still hang on to the “classic” understanding of shared responsibility: the other party will take care of it. For instance, the MDM views the medical device as a “black box” that is expected to be deployed in a secure network without further definition of what those expected network controls are. This may result in device-based security controls not receiving the necessary priority in the design of such products. On the other side, an HDO expects medical devices to be ready for deployment in zero-trust networks with a full and current suite of built-in security controls to defend the device against today’s persistent and aggressive attackers. Indeed, there may even be an assumption that the security controls are equally as robust as the clinical functionality. It is necessary to identify security gaps and document the middle ground that results in medical devices with appropriate security that, when incorporated into an appropriately protected network environment, can be operated at a low-risk level. These two control sets, contained in the device and in the infrastructure, need to complement each other and work together seamlessly. Just as the cyber environment continues to evolve, having a clear understanding of what components need to be maintained and who the maintaining party, is essential to avoid unnecessary incidents.

Conti ransomware attack in Ireland

On May 14, 2021, a major ransomware attack hit Ireland’s Health Service Executive (HSE) ministry, taking down IT services across the entire republic. “Initial reports indicated a human-operated ‘Conti’ ransomware attack that had severely disabled several systems and necessitated the shutdown of the majority of other HSE systems.”² “There are serious impacts to health operations, and some non-emergency procedures are being postponed as hospitals implement their business continuity plans.”²

The Conti ransomware attack, launched two months earlier, impacted 3,500 workstations and 32,800 servers resulting in widespread and lengthy disruption of care delivery.³

The first strategic recommendation made by PwC (formerly Coopers & Lybrand, and Price Waterhouse) in its independent post-incident review was to “Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, share health data or access shared health services.⁴ Establish a ‘code of connection’ that sets minimum cybersecurity requirements for all parties and develop an assurance mechanism to ensure adherence.”⁵ The importance of clearly identified task assignments and accountability across all stakeholders cannot be overstressed in reducing the overall risk of failure.



The main goal should be to prevent an attack from happening in the first place. A practical approach to establishing economically reasonable protection is transparency and collaboration for financial and resource investments across the responsible parties. Since it's only a matter of time before some malware or attack strikes the system, it's crucial to thoroughly analyze prior incidents to identify blind spots of missing cybersecurity protections.

Keeping the cybersecurity posture of medical devices at the highest level is technology-driven and a complex business process of structured activities or tasks involving people that secure confidentiality, integrity, availability (CIA) and, thus, the cybersecurity posture for those devices.

2. Responsibility Assignment Matrix

One method of documenting the tasks and task responsibilities is a Responsibility Assignment Matrix (RAM).⁶ The example in Figure 2 shows how the responsible parties may vary depending on the type of support agreement. Notice that the tasks do not change. The party responsible for fulfilling the task changes with the type of service engagement. This example model is often found with cloud providers, and the responsible party may change depending on whether the infrastructure is maintained on-premise (OnPrem) by the customer or what level of cloud services are contracted; Infrastructure (IaaS), Platform (PaaS), or Software (SaaS).

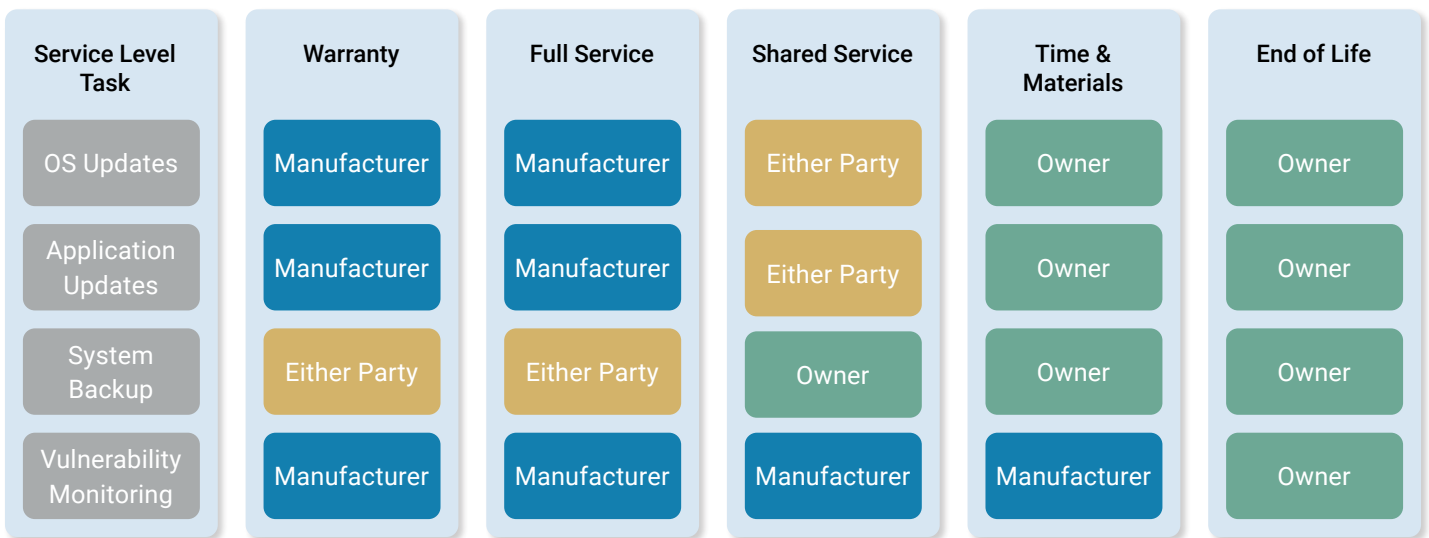


Figure 2. Service based responsibility assignment matrix

One commonly used and proven method to define roles and responsibilities is the Responsible, Accountable, Consulted, and Informed (RACI) matrix. A RACI matrix lists all relevant responsibilities or tasks on one axis and job functions or roles on the other. The RACI matrix uses four key stakeholder responsibilities to identify the level of involvement each party has in any given task. The **Responsible** party is who performs the work. The **Accountable** party is responsible for the decision being made and is held responsible for task completion. The **Consulted** party's input is sought prior to a decision being made or action being taken. The **Informed** party is kept abreast of the decision made or task completion.





The RACI is very useful in concisely identifying each stakeholder’s responsibilities. This information may already be contained in existing documentation or artifacts, such as purchase contracts, service level agreements, instructions for use, operating manuals, Manufacturer Disclosure Statement for Medical Device Security (MDS2) forms, security white papers, or other documents that come with the product. These documents may comprise several thousand pages resulting in critical support information being easily overlooked. Additionally, RACI matrices should be dynamic and periodically updated as device life cycles hit certain milestones or support capabilities change. It is important that the RACI be in a place where all parties can easily use and access the document; real-time access is imperative in quickly understanding which stakeholder(s) to engage for any security related issues. Therefore, ‘living it in reality, not on paper’ is key to gaining maximum CIA benefits from this procedural management approach.

3. Responsibility distribution from software solution to cloud service

The remainder of this document describes how to develop and maintain a RACI matrix for individual system deployment. This paper uses a RACI template as a starting point, to describe a methodology to identify security-relevant tasks, identifying the roles, and assign the role responsibilities.

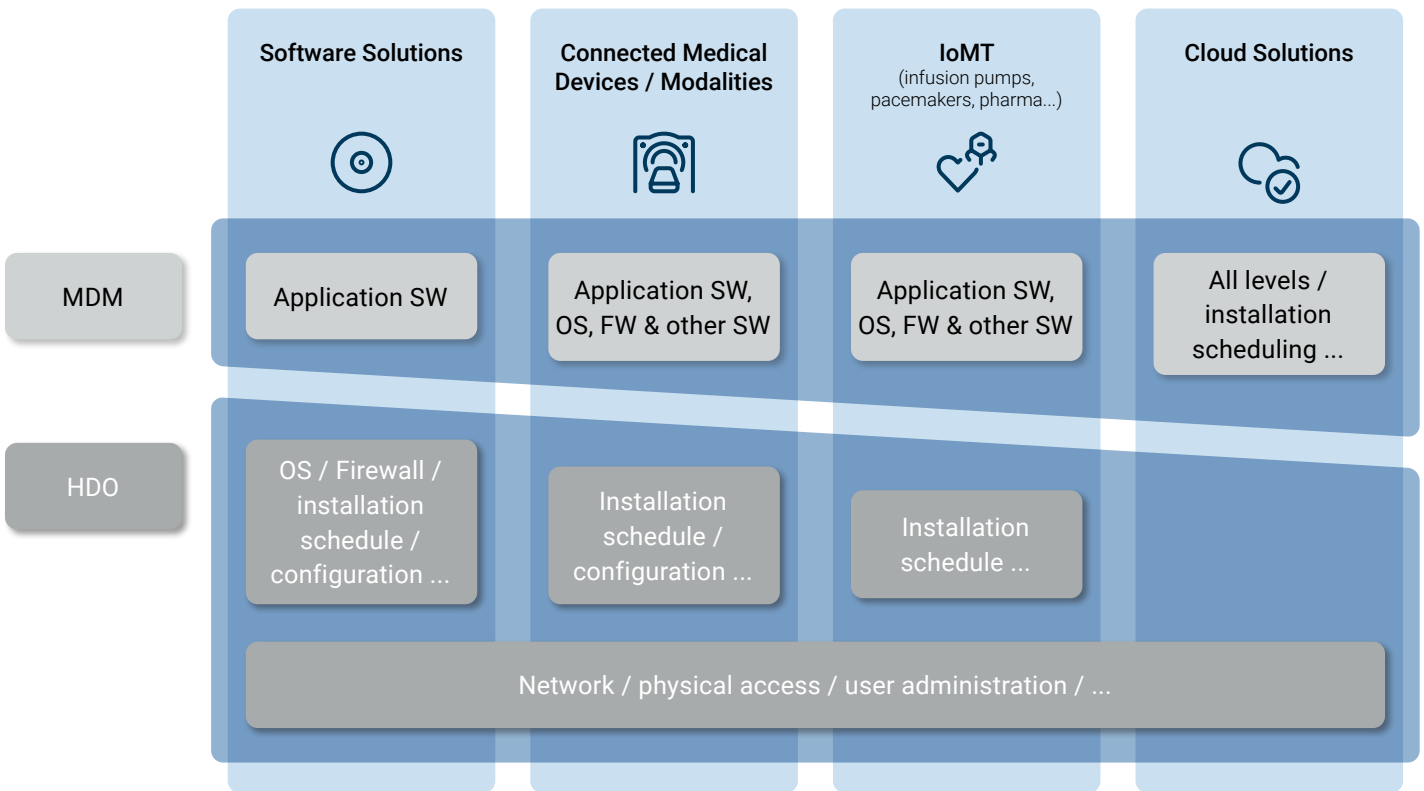


Figure 3. Primary deployment scenarios

The deployment scenarios in Figure 3 depict four security types commonly found in connected medical device environments. This view illustrates how cybersecurity tasks and activities change with each deployment type. With medical devices, there are countless support and deployment combinations. Figure 3 illustrates how each technology's deployment can result in a different distribution of tasks, activities, and responsibilities. The MDM and HDO activity levels change for each medical device security deployment type.

This paper focuses on the shared responsibility matrix for two deployment types from Figure 3, 'Software Solutions' and 'Connected Medical Devices/Modalities.' For discussion purposes, only the MDM and the HDO are identified as stakeholders. In each organization, the tasks may be distributed among one or more teams, but this paper does not explore those additional levels.

Deployment Scenario 1: Software Solutions

When both the MDM and the HDO supply components it is common for each stakeholder to support the components (hardware or software) they provide. In this example, the MDM provides the application software and is responsible for upgrades, updates, patches, and hotfixes to the application software. The HDO provides the network endpoints (hardware or virtual) with the operating system and any required middleware, such as anti-virus protection. The HDO is also responsible for upgrades, updates, patches, hotfixes to the operating system, hardware, memory, processors, middleware, and interfaces. As illustrated, the provider of the component determines the respective responsibility assignments. Keep in mind that different roles and responsibilities may be negotiated and agreed upon for any technology and deployment scenario.

Deployment Scenario 2: Connected Medical Devices/Modalities

For 'Connected Medical Devices/Modalities' the MDM provides both the hardware and software components. The MDM may even provision and configure the device. The HDO is not responsible for maintaining the hardware or software components on the device. This is typically the case while the device is under the manufacturer warranty period. The HDO coordinates installation, configuration, training, upgrades, updates, patches, and hotfixes with the MDM internal service teams. As with Software Solutions, the provider of the components determines the respective responsibility assignments. If the HDO is trained and competent, they may want to assume some of the maintenance tasks. Both parties should identify the needed tasks and agree upon role responsibilities. This negotiation and transfer of responsibility is very important as devices approach end of life and end of support milestones.

Note: This paper omits a process for developing a defined RACI responsibility matrix for the 'IoMT' and 'Cloud Solutions' deployment types since the approach is made visible with 'Software Solutions' as well as 'Connected Medical Devices' already.



4. Procedure to identify and describe defined responsibilities, set up a RACI matrix, and a continuous improvement cycle

There are five major steps to creating and maintaining a RACI. The first step of defining RACI roles at an organizational level need only be done once and then periodically reviewed and updated as appropriate to stay current with organizational norms. The fifth step, a RACI review and revision are typically driven by deployed life cycle milestones such as warranty expiration, key staff changeover, or end of life/end of support milestones. The five steps are listed:

1. Define each RACI role at the organizational level.
2. Identify the tasks or activities associated with supporting the cybersecurity components.
3. List roles and assign stakeholders who may be called upon to perform the cybersecurity tasks. These can include team members, managers, external parties, or any person with a vested interest.
4. Communicate the RACI chart with everyone involved in a task or activity. Make sure that everyone understands their roles and responsibilities.
5. Review and revise the RACI chart periodically to make sure the RACI chart is accurate and up to date.

This paper focuses primarily on steps two through four, which are to list the tasks needed to support the cybersecurity components of the system, identify the responsible party assignments, and share the RACI with stakeholders. This paper limits the stakeholders to the MDM and HDO.

Step 1: Define RACI Roles

Having defined RACI roles enables all stakeholders to understand their role as well as the roles of other stakeholders. This is typically done at the organizational level and remains the same regardless of the medical device a RACI is applied to.

The **Responsible** role is the one who will make sure the work gets completed. This is often the person or team which performs the work. The responsible person needs to know the resource requirements and the time frame for completion. There is only one responsible role assigned per task.

The **Accountable** role is responsible for authorizing the work and determining the work was completed successfully. This includes deciding the work needs to be completed, the identification and/or allocation of resources, and establishes the timeline for completion. There is only one accountable role assigned per task.

The **Consulted** role provides needed input. Depending on the task, the input may be operations, business, risk, or technical in nature and may come from more than one consultant. Consultant role should contribute to a good decision or outcome. There may be more than one consultant role assigned to a task.

The **Informed** role will be notified when the decision to proceed is made and when the work is completed. There may be more than one informed role assigned to a task.



Step 2: Identify the Tasks

Task identification is an essential step in developing a RACI matrix. This step identifies all the tasks critical to maintaining the device's or system's cybersecurity health. Review the architecture to determine the components which may need to be maintained. These include the OS, clinical applications, interfaces, configuration settings, antimalware, and other hardware and software components.

It is helpful to frequently review completed cyber tasks for operating and maintaining medical devices and solutions to optimize operational workflows, detect blind spots or gaps, and identify unclear responsibilities. Additionally, reviewing cybersecurity incidents, performing root cause analysis, and recognizing business case failures are helpful for identifying process and responsibility gaps during the development and review of a RACI matrix.

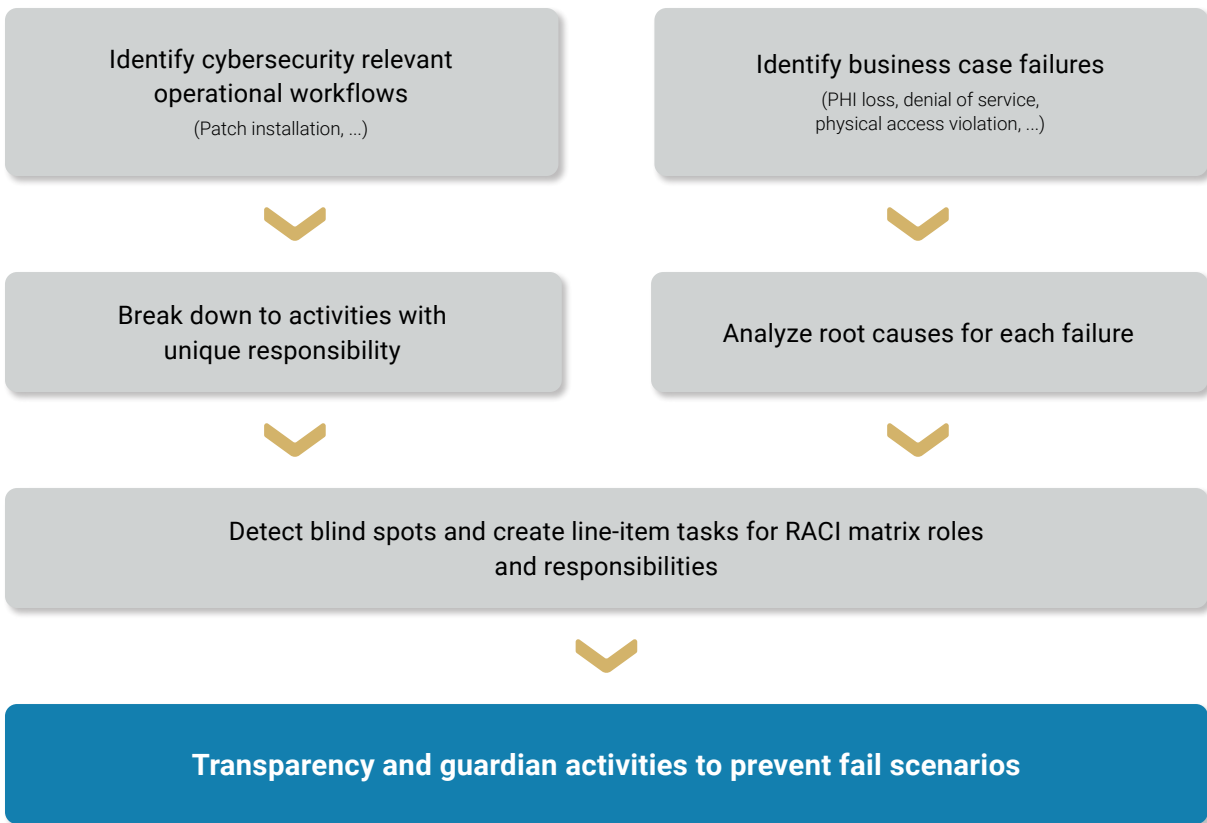




Figure 4. Operational workflow (left) and business case failure (right) evaluation paths to bring transparency for defined responsibilities





Operational workflow

Table 1 provides side-by-side comparison examples of the tasks needed in the process to handle patching the Operating System, secure the Universal Serial Bus (USB), and manage user authentication for the Software Solution and Connected Medical Device deployment scenarios.

Deployment Scenario	 <p>Software Solution on-premise (HDO is responsible for operating system, Commodity-Off-The-Shelf, middleware, and infrastructure)</p>	 <p>Imaging modality system or Intravenous diagnostics (IVD) device (HDO is responsible for installation scheduling and network)</p>
Component	Task	Task
<p>Operating System (OS) security patch:</p>	<ol style="list-style-type: none"> 1. Published OS vulnerability (with or without manufacturer’s vulnerability evaluation). 2. OS published security patch/update to remediate the vulnerability. 3. HDO obtains patch from OS manufacturer and performs installation. <p>> System is running on latest update/patch version fixing the vulnerability.</p>	<p>1. Device OS is supported:</p> <ol style="list-style-type: none"> a. Published OS vulnerability and manufacturer evaluation. b. OS manufacturer and later the MDM publish security patch/update to remediate the vulnerability. c. Remote patch uploaded to system. d. Pop-up window shows available patch. e. HDO performs installation. <p>> System is running on latest update/patch version fixing the vulnerability.</p> <p>2. Device OS is unsupported:</p> <ol style="list-style-type: none"> a. Published OS vulnerability. b. No OS manufacturer and no MDM patch evaluation and release. c. No update/patch from the MDM. <p>> HDO risk assessment and remediation in the form of a compensating control is required to mitigate the vulnerability.</p>





<p>Universal Serial Bus (USB) port security:</p>	<ol style="list-style-type: none"> 1. Customer deactivates USB ports or secures USB ports with physical USB locks. 2. Physical access to the machine via USB port is protected in case of perpetrator/malware trying to access or contaminate the system. 3. In case of allowed USB port usage, protection can be deactivated or temporarily taken off by an HDO or MDM administrator. <p>> USB port HW security lock to access based on designated use cases.</p>	
<p>User Authentication:</p>	<ol style="list-style-type: none"> 1. Advanced authentication (tab on card, biometrical) can be installed on OS. <p>> Applying advanced authentication is the HDO responsibility.</p>	<ol style="list-style-type: none"> 1. System provides username/PW authentication feature. 2. Enable security feature. <p>> Applying regular authentication is the HDO responsibility (if advanced authentication is not available).</p>

Table 1. Operational workflow

Notice that in both deployment scenarios and for each of the three component examples, the HDO is responsible for performing the work. For the Medical Device OS example, the Accountable role changes depending on whether the OS is supported or not. For the supported OS, the MDM evaluates the OS OEM patch and authorizes the HDO to install it. The MDM is the Accountable role in this example. For the unsupported OS, the MDM has no role. The HDO assumes the Accountable role and consultant roles may be called upon to perform risk assessments, replacement estimation or other tasks to enable an informed decision.

Business case failure

Business Case Failure analysis and Root Cause Analysis also provide insights where gaps in tasks and role responsibilities exist. Figure 4 illustrates a top-down root cause analysis tree methodology for an exploited, non-patched OS vulnerability in a connected medical device/modality. Beginning with OS patch availability, the tree identifies decision and outcome tiers to determine possible scenarios and outcomes so proper management techniques can be applied.



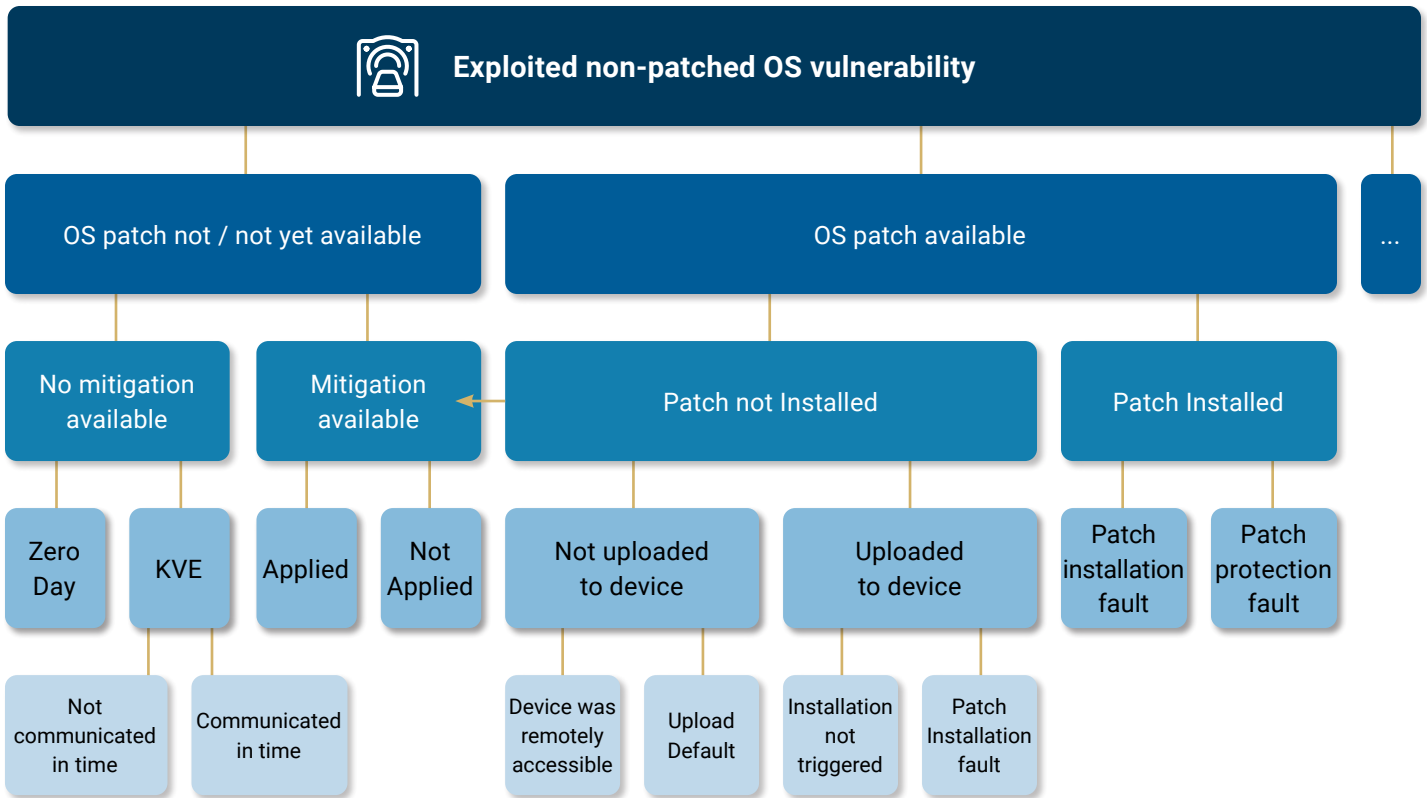


Figure 4. Root Cause Analysis (RCA) tree methodology example.

The tree diagram displays the causation paths for various outcomes. Corrective action, newly required roles or responsibility modifications for an optimized process can be derived from further analyzing the boxes at the bottom of the tree.

Using the techniques of task identification, operational workflow analysis and root cause analysis, help identify the activities and responsibilities for the initial setup, operational procedures, maintenance activities, and support tasks required during the device’s lifecycle. At this point only tasks and activities have been identified. No roles have been assigned as illustrated in Table 2.

Tasks	Team 1	Team 2	Team 3	Team 4
Secure Configuration				
OS Patching				
Clinical Application Update				
Interface Updates				
Remote Access Control				

Table 2 RACI example of tasks only



Granularity

The level of detail, that is, the tasks and subtasks to include in a RACI matrix, is determined by several factors. Refer to the initial goals and priority statements to establish the target level of detail. Next, consider the several tasks required to keep medical devices up-to-date, operational, and safe. Each organization should develop a minimal group of tasks that might be applied across the broadest spectrum of device technologies, understanding that the level of task granularity may vary for the specific technology addressed. For instance, the operating system, clinical applications, interfaces, and protective products such as anti-malware may need to be updated or patched, and one or more teams may support these various software components. More complex systems may demand increased granularity in tasks. For instance, a networking team may keep the anti-malware library up to date while the Healthcare Technology Management (HTM) team is responsible for updating the scanning engine.

Organizational structure may also influence task granularity. The organizational structure at a national or international level may dictate how operational teams interact to maintain the cybersecurity level of medical devices.

For example, manufacturers with an international or global presence might have local, national, continental, headquarters, and customer care centers interacting semi-autonomously or independently, performing product development, sales, and service. Consider this complexity when developing the defined responsibility roles in a RACI matrix. A general recommendation could be to start with basic RACI matrix process responsibility definitions as a template for your organization. Refine and iterate the level of detail for the modality, the solution type, the device architecture, and customer support level options. Revisit and update the RACI matrix periodically to keep current with the medical device lifecycle phase and improvement iterations. Product level RACI matrices may be adjusted as the maturity level and support requirements of the organization evolve as well.

Step 3: List roles and assign stakeholders

The third step in developing a RACI is identifying and assigning the stakeholder responsibilities. Consider creating a template RACI including all possible stakeholders for all possible technologies that a RACI may be applied to in your organization. You may eliminate unneeded roles for RACIs pertaining to specific technologies. Do not name specific people or organizations at this time. Vendor or MDM may be used to represent external parties. Remember, in this paper only the HDO and MDM are identified stakeholders for simplicity of illustration.

Normally you would consider and list all the stakeholder roles in the MDM product development and support teams and in the clinical care environment roles for the HDO. The MDM may condense the HDO roles to a few generalized roles for an MDM-centric RACI matrix. Conversely, the HDO may reduce the MDM view to a few roles for an HDO-centric RACI matrix. A useful technique to identify gaps in tasks, roles, or understanding is to review the RACI with your outside stakeholders.

In addition to the decision makers and the activity doers, be sure to consider the stakeholders who may provide valuable information or will need to be kept abreast of the activities. These are the Consulted and Informed roles. Each organization should identify the roles and responsibilities that each role plays in both operational and maintenance cycles, keeping in mind that not all roles are needed for each technology.

MDM roles

A medical device manufacturer will find the responsibility assignment roles throughout the organization in product development teams, sales teams, service support, and corporate level teams such as legal, risk management, quality, regulatory affairs, and customer service among others.

Sales/account management teams communicate product design features, definitions, tender questionnaires, or other cybersecurity customer requirements. Quality and regulatory affairs provide input for the design and implementation of compliant and quality-assured security controls. Product development teams define cybersecurity process features such as ease of patch update. Legal departments are a good source for cybersecurity terms and conditions, contractual definitions, cybersecurity terms and conditions, and transferability. Transfer discovered requirements into an operational RACI matrix.

In the post-sales phase, specialty groups such as project coordinators, installation engineering, and customer service and support teams play essential roles in using the RACI-defined responsibility tasks in an operative situation. Details of the cooperation between all involved functions must be defined, understood, and communicated to each party's internal organization.

HDO roles

Like the MDM, there are many HDO teams involved in supporting medical devices and clinical technologies. In addition to the traditional Information technology roles, Healthcare Technology Management, facilities management, clinical and business leaders, vendors, and application teams may all play a role in the decision-making or support of clinical care technologies.

Clinical leadership is represented by a caregiver dependent on clinical technology to perform their duties. Depending on the technology, this may be a physician, nurse, technologist, or other direct care providers. Business leadership is responsible for the operations of the clinical care delivery service such as surgical services, imaging services, clinical diagnostics, respiratory, or other therapeutics. Application teams are responsible for ensuring clinical technologies can exchange data with other clinical or business applications and services.

Healthcare Technology Management, also called clinical engineering or biomedical engineering, is responsible for maintaining the operational readiness of clinical technologies. The vendor for clinical technologies typically refers to a party responsible for maintaining the device's or system's operational readiness. A vendor may be the MDM, sometimes referred to as the Original Equipment Manufacturer (OEM), or another third-party service group.

Note: Even if the technology is maintained by the Original Equipment Manufacturer or other third parties, identify the internal group responsible for maintaining device availability.

Information Technology support may include several specialty groups, including End User Computing, Network team, Backup & Storage, Help Desk, Server Group, End User Management, and IT Security. Depending on the technology, not all roles may be involved in device or system support.



Tasks	HDO Technology	HDO Clinical	MDM Product	MDM Support
Secure Configuration	RA	I	C	
OS Patching	C	I	A	R
Clinical Application Update	I	A	C	R
Interface Updates	R	A	C	
Remote Access Control	RA	C		C

Table 3. RACI basic example with tasks and roles

Table 3 illustrates a RACI with responsibilities assigned to stakeholders. Note that every task has only one Responsible (doer) and Accountable (decision maker) stakeholder assignment.

Step 4: Communicate the RACI to all stakeholders

Creating, updating, and sharing the RACI matrix is essential for it to be a useful and valued tool in any organization. Establishing an easy-to-use format and a practical way of sharing the RACI content is vital. Processes for distribution to each party, frequent usage, and predictable updating of this ‘living document’ needs to be established and propagated to all responsible stakeholders. Furthermore, the matrix needs to be used in daily operations to bring the most value.

Detailed information published in the appropriate instructional artifact is a perfect solution. But for quick and easy access, dynamic approaches are needed to keep pace with the changing environment. Some may consider it sufficient that high-level cybersecurity information that defines roles and responsibilities is contained in static contract frameworks, operational manuals, service documents, security white papers, or other attachments. In that case, the commonly used media like RACI developed in Microsoft Excel and shared as a portable document format (pdf) may be sufficient. As maturity, scale and dependency grow, developing into a web tool or even an automated database-sharing approach may make more sense.

A useful appendix to a RACI is a contact list. This is especially useful when external stakeholders such as MDMs, vendors, or 3rd party service providers have roles in maintaining the devices. Large hospitals may have five hundred or more manufacturers represented in the medical device inventory. Having a list of technology specific contacts can save time and frustration when responding to a service event whether planned or not. Review this contact list whenever the RACI is used or reviewed to keep it current.



Step 5: Review and update

A lot of stakeholder engagement is required for setting up and using a RACI matrix approach in daily operations within and across the organization. A commitment from top management down to the operational level folks is the most crucial factor in determining success in improving the confidentiality, integrity, and availability of medical devices. The program and the RACI matrices must also be maintained and improved to adapt to constantly changing environments of involving operational processes, tasks, roles, and responsibilities of all stakeholders resulting in a modified RACI. For example, including blind spots detected over time or eliminating unnecessary action items. Support teams may also experience changes in staff capabilities and responsibilities over time. To ensure the value of an up-to-date RACI matrix, periodically review the baseline and organizational template.

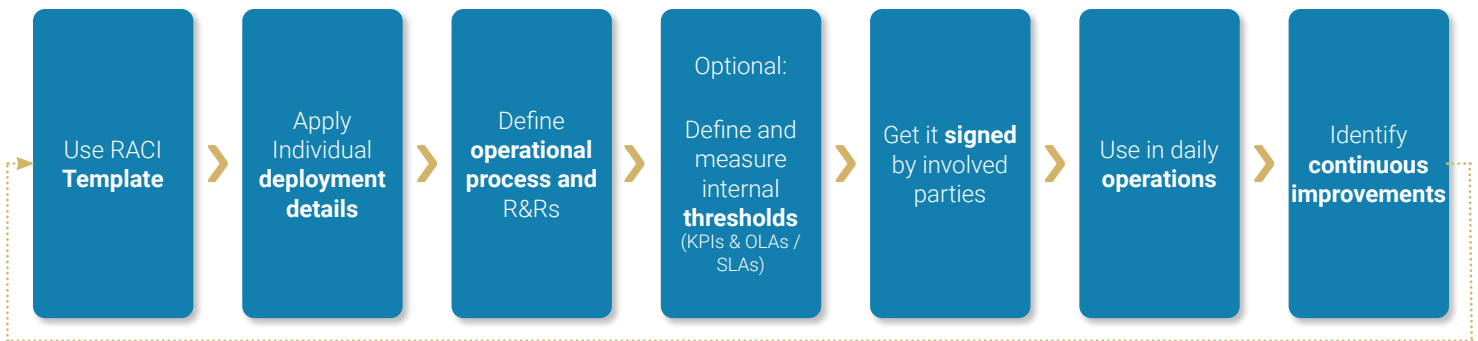


Figure 6. Flow chart for continuous RACI improvement

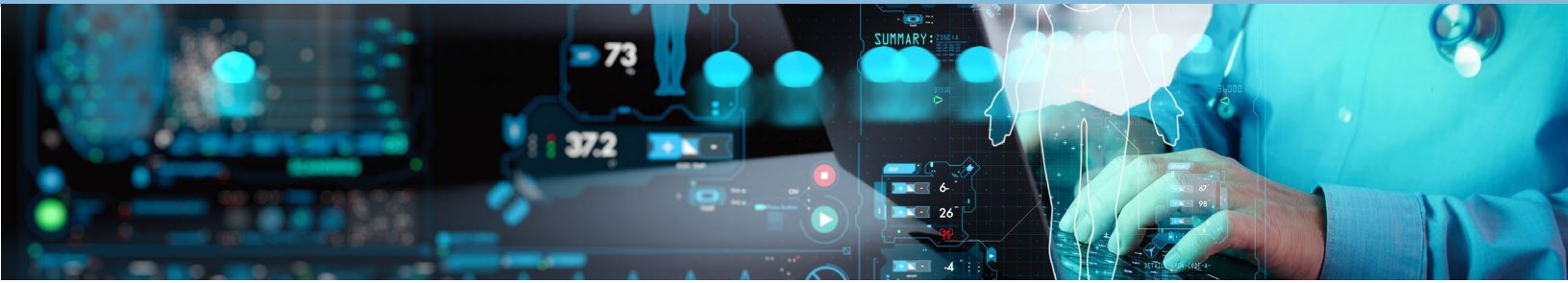
Ideally, RACI matrixes are “living work/checklists” for daily operations. The tasks and responsibility assignments are also useful to define key performance indicators for operational/service level agreements (OLA/SLA). An example could be the work list/process of an HDO biomed department and the scheduled installation of an available cybersecurity update appearing on the medical device user interface.

Wrap up

Successful operational management starts with understanding tasks, roles, and responsibilities. A responsibility assignment matrix is a commonly used methodology to define and manage the cooperative agreement between support entities and stakeholders. In most industries, RACI assignments are negotiated between parties, each striving to maximize the benefits for their organization. The complex nature of the connected medical device environment in the healthcare sector necessitates that responsibilities do not simply allow a change as a stakeholder pleases. Therefore, going forward, the healthcare industry will have no choice but to clearly define the responsibilities of all stakeholders in day-to-day operations to comply with regulations and ultimately increase the confidentiality, integrity, and availability of medical devices for patient safety. Identifying the tasks needed to maintain the cyber health of medical technologies and ensuring there is responsibility assignment and accountability will help ensure healthcare practitioners have secure medical devices with which to provide safe patient care.

Call to Action

Use this [RACI](#) template with example line items derived from different resources for the different action items in the lifecycle of several deployment types to create your RACI matrix.



Appendix 1

MDM RACI example

Building on the foundation previously described, three RACI examples are provided demonstrating an increased task granularity. The increased granularity coincides with the increased level of detail needed by various specialized teams. Using the basic medical device lifecycle, the RACIs progress from high level tasks to more detailed tasks to illustrate how multifaceted teams might use a more detailed RACI to assign responsibilities within a team or smaller sets of teams.

A medical device product life cycle is used at the highest level to identify tasks involved in product component management and can be described in five phase:

1. Product Development

- Concept, Planning, Requirements, Design

2. Deployment and Installation

- Implementation, Verification and Validation, Release Production, Sales

3. Operations and Maintenance

- SBOM Maintenance, Post Market Surveillance, Risk Management, Coordinated Disclosure, Software Updates

4. Incident Management

- Monitoring, Response, Restore, Recovery

5. End of Use

- End of Support, End of Life, decommissioning, disposal



The high level RACI, in Figure 6, illustrates a matrix of vertically arranged basic tasks and horizontally arranged MDM and HDO roles for four deployment types. There are no line-item tasks assigned to any of the stakeholders for this high level view.

Cybersecurity RACI Matrix template draft examples		Security Deployment Scenario											
		Software Solution						Connected Medical Device / Modality		IoMT		Cloud Solutions	
		HDO			MDM			HDO	MDM	HDO	MDM		
		Biomed	IT	Clinical	Deploy/ Install	Service	Product Development		
5	PRE (Product Development)												
12	Deployment / Installation												
13	Networking (LAN)												
14	Firewall configuration												
15	OS Licensing												
16	AiLo licensing												
17	Data base licensing												
18	Secure configuration												
22	Malware protection												
23	Disaster recovery platform												
24	...												
26	Operations / Maintenance												
28	Vulnerability Management												
32	Security risk mitigation												
41	Patching												
107	Network Security												
119	IAM												
134	Backup												
138	Recovery/ Disaster recovery												
141	...												
143	Incident Management												
144	Response												
148	Forensics												
152	Evidence												
155	Reporting												
159	...												
161	POST (EoL, Data and Device Disposal)												

Figure 6. RACI matrix example.



As an example, let’s explore the next level down for the patching task (Figure 6, row 41) under the ‘Operations/Maintenance,’ task heading (Figure 6, line 26). Look ahead to Figure 7, rows 45, 63, 70, & 72 for examples of how the patch delivery methods listed below might appear in a RACI matrix.

The illustration is further simplified by restricting the deployment scenarios to Software Solutions and Connected Medical Devices.

There are the four major patching option methods:

1. MDM delivers the patch over a secure remote connection and either initiates the patch or the patch update is triggered by the operator.
2. HDO is downloading the patch and installing it to the equipment.
3. MDM onsite service team is bringing the patch and installing it to the equipment (with or w/o valid maintenance contract.)
4. Third party onsite service team patch activity.

Here, the patching tasks and subtasks are further broken down for two components, the OS and the application. This example of a shared responsibility RACI matrix focuses on a single patching method ‘a. MDM is patching ...’ is illustrated. Figure 7 illustrates how one common matrix might be used for all HDO and MDM involved tasks and all deployment types. Focusing on Figure 7, we see that patching (Figure 7 row 41) is further delineated to software component types, in this case, Application, (Table 7, row 54). The patching tasks are then further delineated by delivery methods, in this case, via an MDM remote connection, (Figure 7 row 55). The MDM delivery task method can then be broken into specific subtasks, (Figure 7. rows 56-62). Each layer of granularity provides additional opportunity to remove any ambiguity for what tasks are required, and who the responsible party is.

Application

Cybersecurity RACI Matrix template draft examples		Security Deployment Scenario							
		Software Solution						Connected Medical Device / Modality	
		HDO			MDM			HDO	MDM
		Biomed	IT	Clinical	Deploy/Install	Service	Product Development
26	Operations / Maintenance								
41	Patching								
54	Patching options - APPLICATION:								
55	a. MDM remote connection patching:								
56	Allow installation of available security patches within due time, irrespective of whether the patch has been made available based on contract, law or on voluntary basis.	R	C	A				R,A,C	
57	Upload / Push patch to device as soon as available	I			R,A			I	R,A
58	Notify about available security patch in device display or else	I			R,A			I	R,A
59	If there is a delay, inform next level role	I			R,A			I	R,A
60	Schedule patch installation with clinical workflow and MDM	R,A		C		I		R,A,C	I
61	Install patch within due time/ without delay in accordance with respective installation instructions of MDM (semi-automatic patching only)	R				A		R	A
62	Have a fallback patch process / service personal in place in case the remote patching fails	R				A		R	A
63	b. Customer portal patch self-download and self-installation:								
70	c. MDM customer services onsite visit with/ without appropriate and active device maintenance contract:								
72	d. 3rd party customer services onsite visit:								

Figure 7. Application SW patching.



Operating System (and middleware)

Cybersecurity RACI Matrix template draft examples		Security Deployment Scenario									
		Software Solution						Connected Medical Device / Modality			
		HDO			MDM			HDO	MDM		
		Biomed	IT	Clinical	Deploy/Install	Service	Product Development		
92	Patching - OPERATING SYSTEM (OS), firmware (FW), 3rd party SW										
93	Upgrades and Updates of firmware / OS										
94											
95											
96											
97											
98	Patching / Hot Fixing of firmware / OS										
99											
100											
101											
102											
103	Virus Scanning										
104											
105											

Figure 8. Operating System and relevant 3rd party SW patching.

Legend <small>(according to https://en.wikipedia.org/wiki/Responsibility_assignment_matrix)</small>	
R	Responsible (is doing the work)
A	Accountable/Approver (approves the work of responsible)
C	Consultant (Subject Matter Expert counsel)
I	Informee (kept up-to-date)

Figure 9. RACI legend.

Note: For deployment scenario ‘Software Solutions’, the MDM focus is on servicing only the application SW, for deployment scenario ‘Connected Medical Devices/Modalities’, the MDM responsibility also includes the operating system and relevant 3rd party software the HDO is not responsible for.

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email at contact@h-isac.org



Definitions:



Medical device:

“A medical device can be any instrument, apparatus, implement, machine, appliance, implant, and reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination for a medical purpose”. World Health Organization: https://www.who.int/health-topics/medical-devices#tab=tab_1

“Medical devices are products or equipment intended for a medical purpose. In the European Union (EU) they must undergo a conformity assessment to demonstrate they meet legal requirements to ensure they are safe and perform as intended.” European Medicines Agency: <https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices>

References:

- 1 MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices, December 2019 July 2020 rev.1, https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf
- 2 Irish National Cyber Security Centre (NCSC.ie) Report (Conti Ransomware attack 2021) https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf
- 3 Department of Health hit by cyberattack similar to that on HSE. <https://www.irishtimes.com/news/health/department-of-health-hit-by-cyberattack-similar-to-that-on-hse-1.4566541>
- 4 PWC Cyber Threats 2021, A Year in Retrospect <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf>
- 5 Conti cyber-attack on the HSE, PWC December, 2021 [conti-cyber-attack-on-the-hse-full-report.pdf](https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf)
- 6 [RACI-WIKIPEDIA] https://en.wikipedia.org/wiki/Responsibility_assignment_matrix