SECURITY RISK ASSESSMENT FRAMEWORK FOR MEDICAL DEVICES

a **Medical Device Privacy Consortium** *White Paper*

Introduction

The Medical Device Privacy Consortium (MDPC) is a group of leading companies addressing health privacy and security issues affecting the medical device industry.[1] Members of the MDPC manufacture a diverse range of products, from molecular diagnostics to medical imaging equipment to implantable devices.

In light of rapid advancements in technology and focused attention on medical device security, the MDPC launched a product security working group to monitor, analyze and influence global developments in product security issues and develop practical tools that can be used to improve product security in a medical device company.

This white paper offers a framework to medical device manufactures and developers for assessing security risks in medical devices, as well as implementation guidance, referencing to applicable ISO and NIST support and recommendations for successfully implementing the framework.

Background and Objectives

Before diving into the details of our proposed framework for assessing the *security risks* associated with the use of medical devices, it is necessary to first provide context and articulate our objectives.

Medical devices are unique tools that warrant focused attention when it comes to security risk assessment and management. The Food and Drug Administration (FDA) recognized this fact when it issued its draft guidance on *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, released on June 14, 2013 (FDA Draft Guidance).[2] The FDA Draft Guidance identifies issues relating to cybersecurity that manufacturers should consider in preparing premarket submissions with the aim of providing effective cybersecurity management and reducing the risk that device functionality is intentionally or unintentionally compromised. The FDA Draft Guidance encourages manufacturers to develop a set of security controls to assure medical device cybersecurity to maintain the confidentiality, integrity and availability of information.

Although relevant standards for assessing security risks exist, they lack the necessary focus on medical devices, or generally do not allow for universally understood outcomes, focus primarily on patient safety risks or assess impact (*i.e.*, harm) broadly.

[1] Member companies include Abbott Laboratories, Boston Scientific, GE Healthcare, Medtronic, Philips Healthcare, Siemens Healthcare and St. Jude Medical.

[2] Although the specific "recommendations" contained in the FDA Draft Guidance may change once final guidance is issued, the FDA's general focus on medical device security risk assessment and management will likely remain.

This creates a lack of uniformity around security risk assessment across the medical device industry and even among internal business units. This naturally breeds outcomes around risk assessment that are not universally understood – and at times, not fully appreciated – across the organization's multiple business units (*e.g.*, management, sales, marketing, engineering, etc.), between manufacturers (supply chain) or between manufacturers and customers.

Many of these issues relate to a common problem facing the medical device industry when it comes to assessing the security risks associated with the use of medical devices: probability of occurrence of harm. Unlike the empirical data available supporting likelihood determinations with traditional product quality risk assessments, often there is minimal experiential data on the probability of occurrence of harm specific to medical devices. This is exacerbated by the fact that complaints or adverse events relating to security may not be recognized as security issues, thereby depriving industry of valuable data to assist with probability estimations. This creates difficulties for a single engineer, let alone an entire business or industry, to make informed, accurate and consistent probability determinations.

Therefore, our objective is easily stated: resolve these issues in a way that can be easily adopted by industry and integrate with existing approaches to risk management. To achieve this objective we created a framework that allows for a common methodology to assess security risk across industry by focusing specifically on medical devices and using terminology and principles derived from familiar standards. We created a framework that can apply to all medical devices and systems, new and existing, small and large. Keeping in step with the FDA Draft Guidance, we focused on assessing impact to *information confidentiality*, *integrity*, and *availability*, while providing supplemental guidance on impact to issues salient across all business units, from engineering to marketing to C-Suite. We also provided qualitative probability levels and associated descriptions for developers and engineers to yield a more grounded and actionable assessment of security risk.

Our security risk assessment framework is based on the following core ideas:

- **Device Focused, Using Common Principles**. To create something that would be easily adoptable and familiar, we leveraged the terminology and principles found in related standards (*e.g.*, ISO 14971, NIST 800-30 and 800-53, IEC 80001, OWASP Risk Rating Methodology, and Common Vulnerability Scoring System). This framework only veers from these existing terms where necessary to accommodate issues specific to the medical device ecosystem and/or to achieve our stated objective. However, the principles of ISO 14971, NIST 800-30 and IEC 80001 always apply.

- **All Devices, New and Old, Small and Large**. It goes without saying that this framework is universally applicable to all medical devices, new and old, small and large – from a small monitoring device to a large server farm. Further, the framework is usable throughout the product life-cycle, from concept development through design, manufacturing, use and retirement.

- **Tailored Impact**. The security risk assessment framework focuses on impact to the confidentiality, integrity and availability of information – tailored to the medical device environment. When defining impact levels, the framework considers the impact to the confidentiality, integrity and availability of information in the context of the product assessed. For example, the impact of compromised data availability on a life-sustaining device is potentially more severe than the impact on a reporting system. The MDPC also believes that for an entire organization to appreciate the security risks associated with medical devices, the framework should address impacts of all types resulting from security risks. As a result, the framework provides supplemental guidance on assessing impact to the organization (*i.e.*, financial damage, reputational damage, non-compliance and violations of privacy).

- **Simplified Probability**. Risk estimations should examine, among other things, the likelihood of risk scenarios arising and the likelihood that such situations lead to harm. However, with limited empirical data, accurately and universally assessing likelihood is a problem faced by many in the industry. Still, assessing probability is one of the pillars of risk assessment and it most certainly cannot be ignored. As a result, the framework estimates and defines probability in a qualitative manner, focusing on the ability to exploit vulnerabilities associated with identified risk scenarios. Further, although numerous threat agent and vulnerability factors are described, the framework recommends placing greater weight on the skill required by a threat source, the opportunity and resources required by the threat source and the technical ease of exploiting identified vulnerabilities, as these factors can most accurately be determined by manufacturers without much empirical data. This results in more accurate and repeatable outcomes.

We begin by defining key terms that are used throughout the framework. Then, we explain each step of the framework, providing implementation guidance where appropriate. Finally, we discuss the applicability of the framework to the entire product life-cycle and offer recommendations to maximize the framework's utility.

Definitions

For purposes of this framework, the following terms and definitions apply:

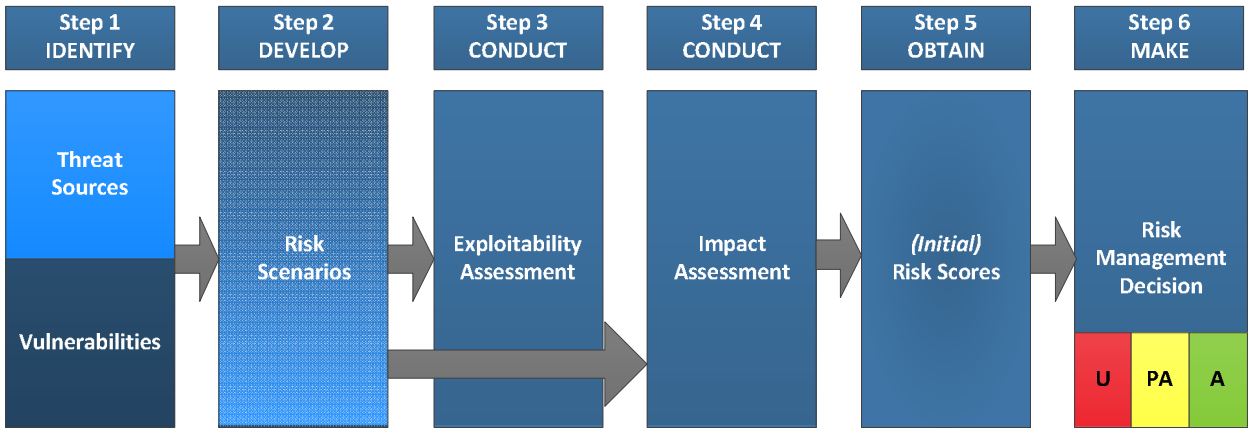
Term	Definition
Exploitability	The ability to exploit all vulnerabilities associated with an identified risk scenario, including the effect of existing security controls.
Hazard	Potential source of harm. *Adopted from ISO 14971.*
Impact	The magnitude of harm that can result from exploiting a risk scenario, including related vulnerabilities and security controls. *Adopted from NIST 800-30 (modified).*
Life-cycle	All phases in the life of a medical device, from the initial conception to final decommissioning and disposal. *Adopted from ISO 14971.*
Medical device	Any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material, or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of: ▪ diagnosis, prevention, monitoring, treatment or alleviation of disease; ▪ diagnosis, monitoring, treatment, alleviation of or compensation for an injury; ▪ investigation, replacement, modification, or support of the anatomy or of a physiological process; ▪ supporting or sustaining life; ▪ control of conception; ▪ disinfection of medical devices; and/or ▪ providing information for medical purposes by means of in vitro examination of specimens derived from the human body. *Adopted from ISO 14971.*
Residual risk	Portion of risk remaining after security controls have been applied. *Adopted from NIST 800-30 (modified).*
Risk scenario	A specific goal or outcome associated with the intentional or unintentional actions of a threat source to exploit vulnerabilities and cause harm. *Adopted from NIST 800-30 definition of "threat scenario" (modified).*

Security controls	The management, operational and technical controls (*i.e.*, safeguards or countermeasures) prescribed for an information system and/or medical device to protect the confidentiality, integrity, and availability of the system and/or device and its information. *Adopted from NIST 800-30 (modified).*
Threat	Any circumstance, event or hazard with the potential to adversely impact individuals (including patients and customers), organizational operations (including mission, functions, image, or reputation), organizational assets (including medical devices) or other organizations. *Adopted from NIST 800-30 (modified).*
Threat source	A person, group, organization, adversarial technology (*e.g.*, malware residing in the cyber environment searching for vulnerabilities) or other threat agent that specifically targets a vulnerability for exploitation, or a situation which occurs or hazard that exists that accidentally exploits a vulnerability. *Adopted from NIST 800-30 (modified).*
Vulnerability	Weakness in an information system, medical device, system or device design, system or device security procedures, internal controls, or implementation that could be exploited by a threat source. *Adopted from NIST 800-30 (modified).*

Security Risk Assessment Framework

Figure 1 illustrates the framework's process for assessing risk in medical devices.

***Figure 1* – Risk Assessment Process**



Step 1: Identify Threat Sources and Vulnerabilities

Identify and document potential threat sources and vulnerabilities relevant to the medical device. To help ensure that all relevant threat sources and vulnerabilities are identified, it is important to enlist the support of security subject matter experts (SMEs) throughout the development process and whenever the framework is applied.

- *Additional guidance on identifying threat sources and vulnerabilities can be found in NIST 800-30 (Ch. 3.2, Tasks 2-1 – 2-3) and ISO 14971 (Ch. 4.2 – 4.4), as well as supporting appendices, annexes and tables.*

- *Additional guidance on identifying hazards can be found in ISO 14971 (Ch. 4.3 – 4.4), as well as supporting appendices, annexes and tables.*

Step 2: Develop Risk Scenarios

Develop and document risk scenarios based on the threat sources and vulnerabilities identified in Step 1. Risk scenarios help focus the assessment on high impact processes, significant vulnerabilities and meaningful threats. Enlist the support of internal and external SMEs to help construct risk scenarios.

- *When developing risk scenarios, it is important to link vulnerabilities with the threat sources that exploit them resulting in harm. This relationship is important in determining the types of security controls that can be applied directly to the vulnerability and the*

mitigating controls that should be considered when the vulnerability cannot be directly addressed through a security control.

- *While not identical, the development of risk scenarios is similar to the identification of hazardous situations under IS0 14971.*

- *Additional guidance on developing risk scenarios can be found in NIST 800-30 (Ch. 2.3.1) and ISO 14971 (Ch. 4.4), as well as supporting appendices, annexes and tables.*

Step 3: Conduct Exploitability Assessment

Assess the ability to exploit vulnerabilities in the identified risk scenarios using the qualitative probability values and criteria set forth in Annex A.

- *The framework does not attempt to quantitatively determine the likelihood of a threat source initiating a threat event and/or the likelihood that such scenarios will adversely impact information confidentiality, integrity, and availability. Instead, the framework focuses on the ability to exploit vulnerabilities in identified risk scenarios based on a qualitative analysis. This results in more accurate and repeatable outcomes.*

- *The framework prescribes four values: 3 (High), 2 (Medium), 1 (Low) and 0 (Validated). The framework describes all four of these values, but gives extra attention to values 3 (High), 1 (Low) and 0 (Validated). Where neither 3 (High) nor 1 (Low) are applicable, the exploitability value will likely be 2 (Medium). An exception to this applies when it would be nearly impossible and/or merely theoretical, even for a highly skilled attacker using advanced equipment, to successfully exploit the vulnerabilities assessed. In these situations, value 0 (Validated) may apply when, among other things, security controls are developed and implemented in a manner that provide a high degree of confidence that the controls are complete, consistent and correct.*

- *Each of the threat and vulnerability factors described in Annex A are relevant when assessing exploitability. However, for values 3 (High), 2 (Medium) and 1 (Low), the framework recommends that manufacturers place greater weight on the skill required by the threat source to exploit vulnerabilities in identified risk scenarios, the opportunity and resources required by the threat source and the technical ease of exploiting identified vulnerabilities. These three factors can most accurately be assessed by manufacturers despite limited empirical data regarding likelihood in the medical device context.*

- *Value 0 (Validated) focuses on the security controls applicable to identified risk scenarios and associated vulnerabilities. Specifically, this value may apply when security controls are developed, implemented and tested in a manner that provide a high degree of confidence that the controls are complete, consistent and correct and as a result, it would be nearly impossible and/or merely theoretical, even for a highly skilled attacker*

using advanced equipment, to successfully exploit the vulnerabilities assessed. Value 0 (Validated) was included after running numerous devices through the framework revealed that it was impossible to obtain an Acceptable risk level (see Step 5 below) when impact was rated 4 (Critical) or 5 (Catastrophic), regardless of the strength and effectiveness of the security controls in place. By including value 0 (Validated), organizations can obtain an Acceptable risk level in these situations. However, this value should only be assigned when all of the descriptions/requirements contained in value 0 (Validated) are satisfied.

- *When assessing the ability to exploit vulnerabilities in existing products, it is important to first consider existing security controls and mitigating factors. Depending on the medical device and its stage in the life-cycle, certain security controls and mitigating factors may already be in place. To the extent that such controls and/or factors address vulnerabilities in identified risk scenarios, their effectiveness must be verified and recorded in the risk management file. Even when existing measures are effective, they only reduce the exploitability of identified risk scenarios. Therefore, relevant risk scenarios must still be evaluated in accordance with the remaining steps of the framework.*

- *The exploitability levels and descriptions contained in Annex A are meant to be flexible and scalable. The framework provides manufacturers with guidance and recommendations, but manufacturers are free to tailor the levels and descriptions as necessary to conform to their environment and devices.*

- *Additional guidance on qualitative probability levels can be found in ISO 14971 (Annex D.3.4), OWASP Risk Rating Methodology and Common Vulnerability Scoring System.*

- *Additional guidance on the implementation of security controls can be found in ISO 14971 (Ch. 6.3) and applicable sections of NIST 800-53, as well as supporting appendices, annexes and tables.*

Step 4: Conduct Impact Assessment

Determine the impact levels of identified risk scenarios using the values and criteria set forth in Annex B.

- *The qualitative impact values contained in Annex B assess impact to the confidentiality, integrity and availability of information in the context of the device assessed, as well as impact on patient safety resulting from a breach to information confidentiality, integrity and/or availability (note, when the impact assessment reveals a potential harmful impact to patient safety, the results of the assessment should be communicated to the relevant safety personnel within the organization and a safety risk assessment should be conducted).*

- *The qualitative impact values also provide supplemental guidance on assessing harm to the organization (i.e., financial damage, reputational damage, non-compliance and violations of privacy). The supplemental guidance is intended to help communicate the meaning and significance of the prescribed impact values across all business units. However, the impact to information confidentiality, integrity and/or availability should always be the focus.*

- *The impact descriptions contained in Annex B are not exhaustive. As with the exploitability levels and descriptions, the impact values contained in Annex B are meant to be flexible and scalable. The framework provides manufacturers with guidance and recommendations, but manufacturers are free to tailor the levels and descriptions as necessary to conform to their environment and devices.*

- *Annex C organizes the descriptions for impact to confidentiality, integrity and availability by impact type (as opposed to impact value). For example, all impact to confidentiality descriptions are grouped together.*

- *Additional guidance on determining impact levels can be found in NIST 800-30 (Ch. 3.2, Task 2-5), as well as supporting appendices, annexes and tables, as well as in the OWASP Risk Rating Methodology and Common Vulnerability Scoring System.*

- *Additional guidance on qualitative impact levels can be found in ISO 14971 (Annex D.3.4).*

Step 5: Obtain *(Initial)* Risk Scores

Combine the exploitability and impact values for each risk scenario in the risk calculator depicted in Figure 2 below to obtain a risk severity score for each risk scenario.

- *The risk score informs the business whether the severity level associated with a certain risk scenario is Unacceptable, Potentially Acceptable or Acceptable.*

- *As explained in Step 6, when the residual risk associated with a given risk scenario is scored Potentially Acceptable, it is highly recommended that manufacturers consider additional security controls or strengthen existing mitigating controls. If and where additional controls are applied, applicable risk scenarios must undergo Steps 3 through 6 again. This cycle must be repeated until (1) residual risk attributable to a relevant risk scenario is scored Acceptable; (2) a decision is made to proceed without additional controls; or (3) the device/project is decommissioned.*

- *As explained in Step 6, when the residual risk associated with a given risk scenario is scored Unacceptable, additional security controls and/or strengthened mitigating controls must be applied unless a decision is made to decommission the device/project. Relevant risk scenarios must repeat Steps 3 through 6 until (1) residual risk is scored*

Acceptable; (2) residual risk is scored Potentially Acceptable and a decision is made to proceed without additional controls; or (3) the device/project is decommissioned.

- *The risk scores are determined at a point in time and may change as a result of an evolving threat and vulnerability landscape. Further, introducing security and mitigating controls may introduce new or different threats and vulnerabilities, thereby leading to additional risk scenarios that will require assessing.*

- *Additional guidance on assessing residual risk and related assessments can be found in NIST 800-30 (Ch. 3.2, Task 2-6) and ISO 14971 (Annex D.4), as well as supporting appendices, annexes and tables.*

***Figure 2* – Risk Level Severity Calculator**

EXPLOITABILITY VALUE	IMPACT VALUE				
	1 (Negligible)	2 (Minor)	3 (Major)	4 (Critical)	5 (Catastrophic)
3 (High)	Potentially Acceptable	Unacceptable	Unacceptable	Unacceptable	Unacceptable
2 (Medium)	Acceptable	Potentially Acceptable	Potentially Acceptable	Unacceptable	Unacceptable
1 (Low)	Acceptable	Acceptable	Acceptable	Potentially Acceptable	Potentially Acceptable
0 (Validated)	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable

Step 6: Make Risk Management Decision

Using the risk severity scores identified in Step 5, determine whether the residual risk attributable to each remaining risk scenario is acceptable or whether additional controls are necessary.

- Where the residual risk associated with a given risk scenario is scored Acceptable, no further evaluation or controls are necessary regarding the Acceptable risk scenario.

- Where the residual risk associated with a given risk scenario is scored Potentially Acceptable, it is highly recommended that manufacturers consider additional security controls or strengthen existing mitigating controls. Where additional controls are applied, applicable risk scenarios must undergo Steps 3 through 6 again. This cycle must be repeated until (1) residual risk attributable to a given risk scenario is scored Acceptable; (2) a decision is made to proceed without additional controls; or (3) the device/project is decommissioned.

- Where the residual risk associated with a given risk scenario is scored Unacceptable, additional security controls and/or strengthened mitigating controls must be applied unless

a decision is made to decommission the device/project. Relevant risk scenarios must repeat Steps 3 through 6 until (1) residual risk is scored Acceptable; (2) residual risk is scored Potentially Acceptable and a decision is made to proceed without additional controls; or (3) the device/project is decommissioned.

- *Introducing security and mitigating controls may also introduce new or different threats and vulnerabilities, thereby leading to additional risk scenarios that must be assessed using the framework.*

- *Additional guidance on the implementation of security controls can be found in ISO 14971 (Ch. 6.3) and applicable sections of NIST 800-53, as well as supporting appendices, annexes and tables.*

- *Additional guidance on residual risk evaluation and risk/benefit analysis can be found in ISO 14971 (Ch. 2.6.4 and 2.6.5), as well as supporting appendices, annexes and tables.*

Life-Cycle Stages

The framework is intended to be equally applicable at all stages of the medical device life-cycle. For new devices, manufacturers are encouraged to apply the framework a minimum of three times: *contemplated design stage*, *mid-development* and *pre-FDA submission*. It is critical to work with engineers throughout the product development life-cycle to develop controls to address known or new vulnerabilities. For existing devices, the framework applies without variation and should be applied on a regular basis depending on the discovery of new vulnerabilities and changes in the threat landscape.

Keys to Success

Based on the collective experiences of MDPC member companies, certain keys to success are clear:

- *Medical device security is more than an IT problem*. In fact, for manufacturers, it's not a traditional IT problem at all. Instead, it is critical that manufacturers obtain support and buy-in from all relevant business units and advisors, including product security teams, SMEs, engineers, developers, design teams, third party integrators and product groups. Manufacturers should also obtain feedback from their representatives in the field who engage with patients and health care providers, and integrate their feedback into devices as appropriate. Although risk acceptance begins with the relevant business unit,

known risks must be escalated and circulated in an easy-to-understand manner so that the appropriate sign-off occurs.[3]

- *Enlist the assistance of security SMEs – both internal and external – whenever applying the framework*. SMEs can help identify threats and vulnerabilities, as well as develop risk scenarios relevant to the medical device at issue. Developing SMEs internally is invaluable, as they provide available and visible problems solvers throughout the device life-cycle.

- *Make product security an asset – not an obligation*. Work with sales and marketing to help sell your security efforts to customers.

Conclusion

This white paper offers a framework to medical device manufactures and developers for assessing security risks in medical devices. We recommend utilizing the framework to efficiently and effectively assess and mitigate product security risks throughout the product life-cycle.

[3] For organizations operating in the user environment, such as health care providers, the IT department is only one of many parties that should be involved in device security. Support and feedback from management, SMEs, third party integrators, those delivering care (*e.g.*, physicians and nurses) and patients themselves is indispensable.

Annex A – Exploitability Values

LEVEL	VALUE DESCRIPTION
3 (High) ***(easy to exploit)***	**Threat Agent Factors** • Skill: Minimal-to-no technical skills required by the threat source(s); unintentional "attack" possible; medical device (and/or network/systems, where applicable) configuration is default and/or utilizes hard-coded passwords. • Motive: Financial or other identifiable gain exists if the threat source(s) is successful. • Opportunity & Resources: No physical access to the medical device (and/or network/systems, where applicable) required by the threat source(s); threat source(s) requires no access rights; no special information (*e.g.*, confidential device or system configuration information) required by the threat source(s); no or low-cost resources required by the threat source(s). **Vulnerability Factors** • Ease of Discovery & Awareness: Vulnerability can be found easily and/or using automated scanning tools, is publicly known or has been exploited previously. • Ease of Exploiting: Vulnerability is easy to exploit and/or can be exploited using automated tools; only off-the-shelf or low-cost equipment necessary, if any. • Intrusion Detection: Intrusion or unauthorized access to the medical device (and/or network/systems, where applicable) is not continuously monitored or logged, logged without regular review (*e.g.*, only during patient visits) or logged and reviewed less than daily. **Effectiveness of Applied Security Controls** • Related security controls are not designed or implemented effectively.

LEVEL	VALUE DESCRIPTION
2 (Medium)	**Threat Agent Factors** • Skill: Advanced computer skills required by the threat source(s); medical device (and/or network/systems, where applicable) configuration is non-default, but commonly configured. • Opportunity & Resources: Some physical access to the medical device (and/or network/systems, where applicable) required by the threat source(s); threat source(s) requires access rights; specialized – but not rare, expensive or difficult to obtain – resources required by the threat source(s). **Vulnerability Factors** • Ease of Exploiting: Vulnerability is difficult to exploit; specialized – but not rare, expensive or difficult to obtain – equipment required by the threat source(s). • Intrusion Detection: Intrusion or unauthorized access to the medical device (and/or network/systems, where applicable) is monitored and logged daily, but no immediate detection mechanism exists. **Effectiveness of Applied Security Controls** • Related security controls are well defined but limited in strength or effectiveness.

Annex A – Exploitability Values (*cont.*)

LEVEL	VALUE DESCRIPTION
1 (Low) ***(difficult to exploit)***	**Threat Agent Factors** • **Skill**: Advanced computer skills in combination with network, programming and/or security penetration skills required by the threat source(s); medical device (and/or network/systems, where applicable) configuration is non-default, not commonly configured and rarely seen publically. • Motive: No financial or other identifiable gain exists if the threat source(s) is successful. • **Opportunity & Resources**: Full physical access to the medical device (and/or network/systems, where applicable) required by the threat source(s); threat source(s) requires elevated/specialized access rights; special information (*e.g.*, confidential device or system configuration information) required by the threat source(s); specialized and expensive resources required by the threat source(s). **Vulnerability Factors** • Ease of Discovery & Awareness: Vulnerability is difficult to discover and has never been exploited previously; vulnerability is unknown or hidden to the threat source(s) identified in the risk scenario. • **Ease of Exploiting**: Vulnerability is nearly impossible to exploit and/or merely theoretical; advanced and/or commercial-grade equipment required. • Intrusion Detection: Intrusion or unauthorized access to the medical device (and/or network/systems, where applicable) is constantly monitored and immediately detected. **Effectiveness of Applied Security Controls** • Related security controls are well defined and multi-layered.

LEVEL	VALUE DESCRIPTION
0 (Validated)	**Threat Agent Factors** • Nearly impossible and/or merely theoretical for a highly skilled attacker using advanced equipment to succeed. **Vulnerability Factors** • Vulnerability is nearly impossible to exploit and/or merely theoretical, even with advanced and/or commercial-grade equipment. **Effectiveness of Applied Security Controls (*all required for value to apply*)** • Security controls are developed and implemented in a manner that provides a high degree of confidence that the controls are complete, consistent and correct. • Security controls meet explicitly identified functional requirements. • Security controls include documentation describing the functional properties, designs and implementation requirements of the controls so as to allow for analysis and testing of the controls. • Security controls continuously and consistently meet their required functions or purposes. • Effectiveness of security controls has been tested, verified and recorded. *"Effectiveness of Applied Security Controls" descriptions are adopted from NIST 800-53 (modified).*

Annex B – Impact Values[4]

IMPACT VALUE: 5 (CATASTROPHIC)		
Primary Assessment – Impact to CIA		
Confidentiality	**Integrity**	**Availability**
• All or a significant number of patient-related records stored on the Device/System and/or Network Systems are disclosed, including patient health information and other sensitive information. • All or a significant number of therapy settings stored on the Device/System and/or Network Systems are disclosed. • All or a significant amount of Device/System-related information stored on the Device/System and/or Network Systems is disclosed, including system structures, configuration settings, passwords and other device settings. • All or a significant amount of other information stored on the Device/System and/or Network Systems is disclosed, including company trade secrets, confidential financial information and other highly-confidential information. • Threat source has complete or a significant amount of control over what information is accessed on the Device/System and/or Network Systems. • Medical and/or personal identity theft resulting in financial harm to patients is highly likely.	• Results in total compromise of Device/System data or integrity and/or Network Systems integrity. • Threat source is able to modify all accessible patient-related records stored on the Device/System and/or Network Systems. • Threat source is able to modify all accessible therapy settings stored on the Device/System and/or Network Systems. • Threat source is able to modify all accessible Device/System-related information, as well as settings associated with Network Systems. • Threat source is able to modify all other accessible information stored on the Device/System and/or Network Systems. • The impact on the integrity of affected information, or Device/System or Network Systems communications, results in a manufacturing system compromise. • Personal data is modified as a result of medical and/or identity theft. • Modification of patient information, therapy settings and/or Device/System-settings results in patient death.	• The Device/System and/or Network Systems are completely shut down and unavailable. • All information, files and records stored on the Device/System and/or Network Systems are unavailable. • Lack of Device/System and/or Network Systems availability results in significant disruption to routine business operations for a prolonged period of time. • Affected Device/System and/or Network Systems are unavailable beyond acceptable levels for most affected systems. • Lack of Device/System and/or Network Systems availability results in patient death.

Supplemental Assessment – Impact to Business			
Financial	***Reputational***	***Non-Compliance***	***Privacy***
• Regulatory fines, remediation costs, breach notification costs and other legal expenses are greater than 20% of operating profit in the current year. • Bankruptcy or near-bankruptcy possible.	• Global media coverage; industry and non-industry publication, blog and news outlet coverage; security incident goes viral. • Irreparable or nearly-irreparable damage to company brand. • Complete or near-complete loss of consumer and patient trust.	• Security incident reveals or results from a clear and alleged-willful violation of federal and international statutes or regulations. • Multi-jurisdictional litigation is certain. • Public hearings are likely or certain.	• Release of sensitive personal data outside the organization impacting greater than 5,000 individuals. • Release of non-sensitive personal data outside the organization impacting greater than 10,000 individuals or individuals from more than 10 states.

[4] *For purposes of this Annex B*, the following terms and definitions shall apply: (1) "Medical Device" or "Device" means the medical device being assessed only, and does not include systems or databases connected to the device; (2) "Device/System" means the medical device being assessed and all systems and databases connected to and supporting the device; (3) "Network Systems" means any and all other systems and databases that can potentially be accessed through the Device/System (*e.g.*, systems and databases that are not entirely segregated from the Device/System).

Annex B – Impact Values (*cont.*)

IMPACT VALUE: 4 (CRITICAL)		
Primary Assessment – Impact to CIA		
Confidentiality	**Integrity**	**Availability**
• Complete access to patient-related records is limited to records stored on the Device/System; threat source has limited access to Network Systems that process patient information. • Complete access to therapy settings is limited to settings stored on the Device/System; threat source has limited access to Network Systems that store therapy settings. • Complete access to Device/System-related information is limited to information stored on the Device/System; threat source has limited access to Network Systems that process Device/System-related information. • Complete access to other information is limited to information stored on the Device/System; threat source has limited access to Network Systems. • Significant amount of sensitive or other critical information is disclosed. • Threat source has complete or a significant amount of control over what information is accessed on the Device/System, but no control over what information is accessed on the Network Systems. • Medical and/or personal identity theft resulting in financial harm to patients is likely.	• Results in significant compromise of accessible Device/System and/or Network Systems data or integrity. • Threat source is able to modify a significant number of accessible patient-related records stored on the Device/System and/or Network Systems. • Threat source is able to modify a significant number of accessible therapy settings stored on the Device/System and/or Network Systems. • Threat source is able to modify a significant number of accessible Device/System-related settings stored on the Device/System and/or Network Systems. • Threat source is able to modify a significant amount of other accessible information stored on the Device/System and/or Network Systems. • The impact on the integrity of affected information, or Device/System or Network Systems communications, could lead to a manufacturing system compromise with risk to Device/System integrity. • Extensive amount of sensitive or other critical information corrupted. • Personal data likely modified as a result of medical and/or identity theft. • Modification of patient information, therapy settings and/or Device/System-settings results in permanent impairment or life-threatening injury.	• Affected Device/System and/or Network Systems are significantly shut down and unavailable. • A significant amount of information, files and records stored on affected Device/System and/or Network Systems are unavailable. • Lack of affected Device/System and/or Network Systems availability results in disruption to routine business operations. • Affected Devices/Systems and/or Network Systems are unavailable beyond acceptable levels for many systems. • Lack of Device/System and/or Network Systems availability results in permanent impairment or life-threatening injury.

Supplemental Assessment – Impact to Business			
Financial	***Reputation***	***Non-Compliance***	***Privacy***
• Regulatory fines, remediation costs, breach notification costs and other legal expenses are between 7% and 20% of operating profit in the current year. • Significant impact on annual profit.	• National media coverage; industry and non-industry publication and blog coverage. • Damage to company brand. • Damage to consumer and patient trust.	• Security incident reveals or results from a clear violation of federal and international statutes or regulations. • Litigation is certain. • Public hearings are possible.	• Release of sensitive personal data outside the organization impacting 501-5000 individuals. • Release of non-sensitive personal data outside the organization impacting 5,001-10,000 individuals or individuals from more 5-10 states.

Annex B – Impact Values (*cont.*)

IMPACT VALUE: 3 (SERIOUS)		
Primary Assessment – Impact to CIA		
Confidentiality	**Integrity**	**Availability**
• Access to patient-related records is limited to information stored on the Device/System, including patient health information and other sensitive information. • Access to therapy settings is limited to information stored on the Device/System. • Access to Device/System-related information is limited to information stored on the Device/System. • Access to other information is limited to information stored on the Device/System. • Extensive amount of non-sensitive information and/or limited amount of sensitive information is disclosed. • Threat source has limited access to information stored on the Device/System and/or Network Systems, and has no control over what information is accessed. • Medical and/or personal identity theft resulting in financial harm to patients is possible.	• Compromise of accessible Device/System data or integrity is possible, but threat source has no control over what information is accessed. • Threat source has the potential to modify accessible patient-related records stored on the Device/System, but has no control over what information is accessed. • Threat source has the potential to modify accessible therapy settings stored on the Device/System, but has no control over what information is accessed. • Threat source has the potential to modify accessible Device/System-related settings stored on the Device/System, but has no control over what information is accessed. • Threat source has the potential to modify other accessible information stored on the Device/System and/or Network Systems, but has no control over what information is accessed. • The impact on the integrity of affected information, or Device/System or Network Systems communications, does not lead to a manufacturing system compromise. • Extensive amount of non-sensitive and/or a limited amount of sensitive information corrupted. • Personal data possibly modified as a result of medical and/or identity theft. • Modification of patient information, therapy settings and/or Device/System-settings results in injury or impairment requiring professional medical intervention.	• Affected Device/System and/or Network Systems are temporarily interrupted or system performance is reduced. • Limited information, files and records stored on affected Device/System and/or Network Systems are unavailable. • The unavailability of affected Device/System and/or Network Systems affects routine business operations but with limited impact. • Affected Devices/Systems and/or Network Systems are unavailable for acceptable durations. • Lack of Device/System availability results in injury or impairment requiring professional medical intervention.

Supplemental Assessment – Impact to Business			
Financial	***Reputation***	***Non-Compliance***	***Privacy***
• Regulatory fines, remediation costs, breach notification costs and other legal expenses are between 2% and 7% of operating profit in the current year. • Minor impact on annual profit.	• Local or regional media coverage; industry publication coverage. • Loss of consumer/patient good will.	• Security incident reveals or results from a potential violation of federal and international statutes or regulations. • Litigation is likely. • Public hearings are not likely.	• Release of sensitive personal data outside the organization impacting 1-500 individuals. • Release of non-sensitive personal data outside the organization impacting 501-5,000 individuals.

Annex B – Impact Values (*cont.*)

IMPACT VALUE: 2 (MINOR)		
Primary Assessment – Impact to CIA		
Confidentiality	**Integrity**	**Availability**
• Access to patient-related records is unlikely and limited to information stored on the Device/System. • Access to therapy settings is unlikely and limited to information stored on the Device/System. • Access to Device/System-related information is unlikely and limited to information stored on the Device/System. • Access to other information is unlikely and limited to information stored on the Device/System. • Limited non-sensitive personal data is disclosed; no sensitive personal data is disclosed. • Threat source has limited access to information stored on the Device/System and no access to Network Systems; threat source has no control over what information is accessed on the Device/System. • Medical and/or personal identity theft resulting in financial harm to patients is unlikely.	• Compromise of accessible Device/System data or integrity is unlikely and threat source has no control over what information is accessed. • Modification of accessible patient-related records stored on the Device/System is unlikely and threat source has no control over what information is accessed. • Modification of accessible therapy settings stored on the Device/System is unlikely and threat source has no control over what information is accessed. • Modification of accessible Device/System-related settings stored on the Device/System is unlikely and threat source has no control over what information is accessed. • Modification of other accessible information stored on the Device/System is unlikely and threat source has no control over what information is accessed. • The impact on the integrity of affected information or Device/System communications does not lead to a manufacturing system compromise. • Limited amount of non-sensitive and no sensitive personal data corrupted. • Modification of patient information, therapy settings and/or Device/System-settings results in temporary and minor injury or impairment not requiring professional medical intervention.	• Affected Device/System is temporarily interrupted or performance is reduced. • Limited information, files and records stored on affected Device/System may be temporarily unavailable. • The unavailability of affected Device/Systems affects routine business operations but with no material impact. • Affected Devices/Systems are unavailable for acceptable durations. • Lack of Device/System availability results in temporary and minor injury or impairment not requiring professional medical intervention.

Supplemental Assessment – Impact to Business			
Financial	***Reputation***	***Non-Compliance***	***Privacy***
• Regulatory fines, remediation costs, breach notification costs and other legal expenses are between 1% and 2% of operating profit in the current year. • No material impact on annual profit.	• Media coverage limited to industry publications. • Loss of significant customers.	• No violation of federal and international statutes or regulations likely; civil or state claims possible. • Litigation is possible. • No public hearings warranted.	• No sensitive personal data is disclosed. • Release of limited non-sensitive personal data outside the organization impacting 500 or less individuals.

Annex B – Impact Values (*cont.*)

IMPACT VALUE: 1 (NEGLIGIBLE)		
Primary Assessment – Impact to CIA		
Confidentiality	**Integrity**	**Availability**
• No access to patient-related records. • No access to therapy settings. • No access to Device/System-related information. • No access to other information. • No personal data disclosed. • Threat source has no access to information stored on the Device/System or Network Systems. • No medical and/or personal identity theft resulting in financial harm to patients.	• No material compromise of Device/System and/or Network Systems data or integrity. • No material modification to patient-related records, therapy settings, Device/System-related settings or other information. • No material impact on the integrity of affected information or Device/System communications and as a result, no manufacturing system compromise. • No personal data corrupted. • Modification of patient information, therapy settings and/or Device/System-settings results in inconvenience or temporary discomfort; no injury to patient.	• No material interruption or performance reduction. • All files and records available. • No effect on routine business operations. • Device/Systems and Network Systems are available at all times. • Lack of Device/System availability results in inconvenience or temporary discomfort; no injury to patient.

Supplemental Assessment – Impact to Business			
Financial	***Reputation***	***Non-Compliance***	***Privacy***
• Costs are less than 1% of operating profit in the current year and/or limited to cost to remediate vulnerability. • No impact on annual profit.	• No media coverage. • Minimal reputational damage.	• No legal violations; limited-to-no civil claims. • Litigation is unlikely or quickly resolved. • No public hearings.	• No personal data is disclosed.

Annex C – Confidentiality, Integrity & Availability Impact Values (*by Category*)[5]

CONFIDENTIALITY				
5 (Catastrophic)	**4 (Critical)**	**3 (Serious)**	**2 (Minor)**	**1 (Negligible)**
• All or a significant number of patient-related records stored on the Device/System and/or Network Systems are disclosed, including patient health information and other sensitive information. • All or a significant number of therapy settings stored on the Device/System and/or Network Systems are disclosed. • All or a significant amount of Device/System-related information stored on the Device/System and/or Network Systems is disclosed, including system structures, configuration settings, passwords and other device settings. • All or a significant amount of other information stored on the Device/System and/or Network Systems is disclosed, including company trade secrets, confidential financial information and other highly-confidential information. • Threat source has complete or a significant amount of control over what information is accessed on the Device/System and/or Network Systems. • Medical and/or personal identity theft resulting in financial harm to patients is highly likely.	• Complete access to patient-related records is limited to records stored on the Device/System; threat source has limited access to Network Systems that process patient information. • Complete access to therapy settings is limited to settings stored on the Device/System; threat source has limited access to Network Systems that store therapy settings. • Complete access to Device/System-related information is limited to information stored on the Device/System; threat source has limited access to Network Systems that process Device/System-related information. • Complete access to other information is limited to information stored on the Device/System; threat source has limited access to Network Systems. • Significant amount of sensitive or other critical information is disclosed. • Threat source has complete or a significant amount of control over what information is accessed on the Device/System, but no control over what information is accessed on the Network Systems. • Medical and/or personal identity theft resulting in financial harm to patients is likely.	• Access to patient-related records is limited to information stored on the Device/System, including patient health information and other sensitive information. • Access to therapy settings is limited to information stored on the Device/System. • Access to Device/System-related information is limited to information stored on the Device/System. • Access to other information is limited to information stored on the Device/System. • Extensive amount of non-sensitive information and/or limited amount of sensitive information is disclosed. • Threat source has limited access to information stored on the Device/System and/or Network Systems, and has no control over what information is accessed. • Medical and/or personal identity theft resulting in financial harm to patients is possible.	• Access to patient-related records is unlikely and limited to information stored on the Device/System. • Access to therapy settings is unlikely and limited to information stored on the Device/System. • Access to Device/System-related information is unlikely and limited to information stored on the Device/System. • Access to other information is unlikely and limited to information stored on the Device/System. • Limited non-sensitive personal data is disclosed; no sensitive personal data is disclosed. • Threat source has limited access to information stored on the Device/System and no access to Network Systems; threat source has no control over what information is accessed on the Device/System. • Medical and/or personal identity theft resulting in financial harm to patients is unlikely.	• No access to patient-related records. • No access to therapy settings. • No access to Device/System-related information. • No access to other information. • No personal data disclosed. • Threat source has no access to information stored on the Device/System or Network Systems. • No medical and/or personal identity theft resulting in financial harm to patients.

[5] *For purposes of this Annex C*, the following terms and definitions shall apply: (1) "Medical Device" or "Device" means the medical device being assessed only, and does not include systems or databases connected to the device; (2) "Device/System" means the medical device being assessed and all systems and databases connected to and supporting the device; (3) "Network Systems" means any and all other systems and databases that can potentially be accessed through the Device/System (*e.g.*, systems and databases that are not entirely segregated from the Device/System).

Annex C – Confidentiality, Integrity & Availability Impact Values (*by Category*)

INTEGRITY				
5 (Catastrophic)	**4 (Critical)**	**3 (Serious)**	**2 (Minor)**	**1 (Negligible)**
• Results in total compromise of Device/System data or integrity and/or Network Systems integrity. • Threat source is able to modify all accessible patient-related records stored on the Device/System and/or Network Systems. • Threat source is able to modify all accessible therapy settings stored on the Device/System and/or Network Systems. • Threat source is able to modify all accessible Device/System-related information, as well as settings associated with Network Systems. • Threat source is able to modify all other accessible information stored on the Device/System and/or Network Systems. • The impact on the integrity of affected information, or Device/System or Network Systems communications, results in a manufacturing system compromise. • Personal data is modified as a result of medical and/or identity theft. • Modification of patient information, therapy settings and/or Device/System-settings results in patient death.	• Results in significant compromise of accessible Device/System and/or Network Systems data or integrity. • Threat source is able to modify a significant number of accessible patient-related records stored on the Device/System and/or Network Systems. • Threat source is able to modify a significant number of accessible therapy settings stored on the Device/System and/or Network Systems. • Threat source is able to modify a significant number of accessible Device/System-related settings stored on the Device/System and/or Network Systems. • Threat source is able to modify a significant amount of other accessible information stored on the Device/System and/or Network Systems. • The impact on the integrity of affected information, or Device/System or Network Systems communications, could lead to a manufacturing system compromise with risk to Device/System integrity. • Extensive amount of sensitive or other critical information corrupted. • Personal data likely modified as a result of medical and/or identity theft. • Modification of patient information, therapy settings and/or Device/System-settings results in permanent impairment or life-threatening injury.	• Compromise of accessible Device/System data or integrity is possible, but threat source has no control over what information is accessed. • Threat source has the potential to modify accessible patient-related records stored on the Device/System, but has no control over what information is accessed. • Threat source has the potential to modify accessible therapy settings stored on the Device/System, but has no control over what information is accessed. • Threat source has the potential to modify accessible Device/System-related settings stored on the Device/System, but has no control over what information is accessed. • Threat source has the potential to modify other accessible information stored on the Device/System and/or Network Systems, but has no control over what information is accessed. • The impact on the integrity of affected information, or Device/System or Network Systems communications, does not lead to a manufacturing system compromise. • Extensive amount of non-sensitive and/or a limited amount of sensitive information corrupted. • Personal data possibly modified as a result of medical and/or identity theft. • Modification of patient information, therapy settings and/or Device/System-settings results in injury or impairment requiring medical intervention.	• Compromise of accessible Device/System data or integrity is unlikely and threat source has no control over what information is accessed. • Modification of accessible patient-related records stored on the Device/System is unlikely and threat source has no control over what information is accessed. • Modification of accessible therapy settings stored on the Device/System is unlikely and threat source has no control over what information is accessed. • Modification of accessible Device/System-related settings stored on the Device/System is unlikely and threat source has no control over what information is accessed. • Modification of other accessible information stored on the Device/System is unlikely and threat source has no control over what information is accessed. • The impact on the integrity of affected information or Device/System communications does not lead to a manufacturing system compromise. • Limited amount of non-sensitive and no sensitive personal data corrupted. • Modification of patient information, therapy settings and/or Device/System-settings results in temporary and minor injury or impairment not requiring professional medical intervention.	• No material compromise of Device/System and/or Network Systems data or integrity. • No material modification to patient-related records, therapy settings, Device/System-related settings or other information. • No material impact on the integrity of affected information or Device/System communications and as a result, no manufacturing system compromise. • No personal data corrupted. • Modification of patient information, therapy settings and/or Device/System-settings results in inconvenience or temporary discomfort; no injury to patient.

Annex C – Confidentiality, Integrity & Availability Impact Values (*by Category*)

AVAILABILITY				
5 (Catastrophic)	**4 (Critical)**	**3 (Serious)**	**2 (Minor)**	**1 (Negligible)**
• The Device/System and/or Network Systems are completely shut down and unavailable. • All information, files and records stored on the Device/System and/or Network Systems are unavailable. • Lack of Device/System and/or Network Systems availability results in significant disruption to routine business operations for a prolonged period of time. • Affected Device/System and/or Network Systems are unavailable beyond acceptable levels for most affected systems. • Lack of Device/System and/or Network Systems availability results in patient death.	• Affected Device/System and/or Network Systems are significantly shut down and unavailable. • A significant amount of information, files and records stored on affected Device/System and/or Network Systems are unavailable. • Lack of affected Device/System and/or Network Systems availability results in disruption to routine business operations. • Affected Devices/Systems and/or Network Systems are unavailable beyond acceptable levels for many systems. • Lack of Device/System and/or Network Systems availability results in permanent impairment or life-threatening injury.	• Affected Device/System and/or Network Systems are temporarily interrupted or system performance is reduced. • Limited information, files and records stored on affected Device/System and/or Network Systems are unavailable. • The unavailability of affected Device/System and/or Network Systems affects routine business operations but with limited impact. • Affected Devices/Systems and/or Network Systems are unavailable for acceptable durations. • Lack of Device/System availability results in injury or impairment requiring professional medical intervention.	• Affected Device/System is temporarily interrupted or performance is reduced. • Limited information, files and records stored on affected Device/System may be temporarily unavailable. • The unavailability of affected Device/Systems affects routine business operations but with no material impact. • Affected Devices/Systems are unavailable for acceptable durations. • Lack of Device/System availability results in temporary and minor injury or impairment not requiring professional medical intervention.	• No material interruption or performance reduction. • All files and records available. • No effect on routine business operations. • Device/Systems and Network Systems are available at all times. • Lack of Device/System availability results in inconvenience or temporary discomfort; no injury to patient.