Technical Information Report

AAMI TIR57: 2016

Principles for medical device security—Risk management

AAMI
Advancing Safety in Healthcare Technology

Principles for medical device security—Risk management

Approved 5 June 2016 by
Association for the Advancement of Medical Instrumentation

Abstract: Provides guidance on methods to perform information security risk management for a medical device in the context of the Safety Risk Management process required by ISO 14971. The TIR incorporates the expanded view of risk management from IEC 80001-1 by incorporating the same key properties of Safety, Effectiveness and Data & Systems Security with Annexes that provide process details and illustrative examples.

Keywords: medical device, information security, risk management

AAMI Technical Information Report

A technical information report (TIR) is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) Standards Board that addresses a particular aspect of medical technology.

Although the material presented in a TIR may need further evaluation by experts, releasing the information is valuable because the industry and the professions have an immediate need for it.

A TIR differs markedly from a standard or recommended practice, and readers should understand the differences between these documents.

Standards and recommended practices are subject to a formal process of committee approval, public review, and resolution of all comments. This process of consensus is supervised by the AAMI Standards Board and, in the case of American National Standards, by the American National Standards Institute.

A TIR is not subject to the same formal approval process as a standard. However, a TIR is approved for distribution by a technical committee and the AAMI Standards Board.

Another difference is that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years. For a TIR, AAMI consults with a technical committee about five years after the publication date (and periodically thereafter) for guidance on whether the document is still useful—that is, to check that the information is relevant or of historical value. If the information is not useful, the TIR is removed from circulation.

A TIR may be developed because it is more responsive to underlying safety or performance issues than a standard or recommended practice, or because achieving consensus is extremely difficult or unlikely. Unlike a standard, a TIR permits the inclusion of differing viewpoints on technical issues.

CAUTION NOTICE: This AAMI TIR may be revised or withdrawn at any time. Because it addresses a rapidly evolving field or technology, readers are cautioned to ensure that they have also considered information that may be more recent than this document.

All standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are *voluntary*, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

Published by

Association for the Advancement of Medical Instrumentation
4301 N Fairfax Drive, Suite 301
Arlington, VA 22203-1633

Printed in the United States of America

ISBN 1-57020-612-0

Contents

Page

Tables

Figures

Glossary of equivalent standards

International Standards or Technical Reports adopted in the United States may include normative references to other International Standards. AAMI maintains a current list of each International Standard that has been adopted by AAMI (and ANSI). Available on the AAMI website at the address below, this list gives the corresponding U.S. designation and level of equivalency to the International Standard.

www.aami.org/standards/glossary.pdf

Committee representation

Association for the Advancement of Medical Instrumentation

Medical Device Security Working Group

The publication of AAMI TIR57 as a new American Technical Information Report was initiated by the AAMI Medical Device Security Working Group.

At the time this document was published, the **AAMI Medical Device Security Working Group** had the following members:

Cochairs:
Ken Hoyme, Adventium Labs
Geoff Pascoe, Deloitte Advisory

Members:
Mike Ahmadi, Synopsys Inc
Pat Baird, Baxter Healthcare Corporation
Andrew Dean, Amgen Inc
Harsh Dharwad, Hospira Worldwide Inc
Sherman Eagles, SoftwareCPR
Scott Eaton, Mindray DS USA Inc
Plamena Entcheva-Dimitrov, Preferred Regulatory Consulting
Charles S. Farlow, Medtronic Inc.Charles Farlow, Medtronic Inc Campus
Phil Fisk, Baxter Healthcare Corporation
Brian Fitzgerald, FDA/CDRH
Alan Fryer, Micro Systems Engineering Inc
Kevin Fu, The University of Michigan
Ken Fuchs, Center for Medical Interoperability
Bill Hagestad, Smiths Medical
Ed Heierman, Abbott Laboratories
Mike Jaffe, Cardiorespiratory Consulting LLC
Michelle Jump, Stryker Instruments Division
Joshua Kim, Hill-Rom Holdings
Insup Lee
Yimin Li, St Jude Medical Inc
Dan Lyon, Cigital Inc
Melissa Masters, Battelle Medical Products
Jill McCormick, Department of Veteran Affairs
Mary Beth McDonald, Mary Beth McDonald Consulting
Michael McNeil, Philips Electronics North America
Dale Nordenberg
Andrew O'Keeffe, Draeger Medical Systems Inc
Brodie Pedersen, Logic PD
Arnab Ray
Larry Schwartz, Smiths Medical
Michael Seeberger, Boston Scientific Corporation
Lynette Sherrill, Department of Veteran Affairs
Ferry Tamtoro, Amgen Inc
Tom Vaccaro, Becton Dickinson & Company
Fubin Wu, GessNet
Daidi Zhong, Chongqing University

Alternates:
Tushar Dharampal, St Jude Medical Inc
Leo Espindle, Amgen Inc
Dawn Flakne, Micro Systems Engineering Inc
Elisabeth George, Philips Electronics North America
Roberta Hansen, Abbott Laboratories
Karen Kazak, Baxter Healthcare Corporation
Tara Larson, Medtronic Inc.

Nick Sikorski, Deloitte Advisory
Nikhil Thakur, FDA/CDRH
J.S. Wiley, Draeger Medical Systems Inc

NOTE—Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

Foreword

This technical information report (TIR) was developed by the Device Security Working Group.

It is widely recognized that there is little existing guidance for conducting cybersecurity risk assessment of medical devices.

The objective of this TIR is to provide guidance on how medical device manufacturers can manage risks from security threats that could impact the confidentiality, integrity, and/or availability of the device or the information processed by the device. Because medical device manufacturers are already familiar with ANSI/AAMI/ISO 14971:2007, this guidance follows the basic structure of that standard.

Suggestions for improving this recommended practice are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

NOTE This foreword does not contain provisions of the AAMI TIR57, *Principles for medical device security– Risk management* (AAMI TIR57:2016), but it does provide important information about the development and intended use of the document.

Introduction

Medical device manufacturers are familiar with the requirements of ANSI/AAMI/ISO 14971:2007/(R)2010 *Medical devices — Application of risk management to medical devices*. This standard is an integral part of the safety risk management processes required by many regulatory authorities. ANSI/AAMI/ISO 14971 specifies a process for a manufacturer to identify the hazards associated with medical devices, including *in vitro* diagnostic (IVD) medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls (see Clause 1 of ANSI/AAMI/ISO 14971:2007).

NOTE In 2012, the European Committee for Standardization (CEN) adopted EN ISO 14971:2012 as the European harmonized standard, superseding EN ISO 14971:2009. This document does not address content deviations included in Annex ZA of EN ISO 14971:2012. Specifically, the "as far as possible" requirement is not included in the evaluation of security risks. Instead, security risks are to be assessed and controlled to a level that is considered acceptable, taking into account the impact of a threat event and potential vulnerabilities.

Specific clauses of ANSI/AAMI/ISO 14971:2007 define a risk management process consisting of the following elements:

- risk analysis (Clause 4);
- risk evaluation (Clause 5);
- risk control (Clause 6);
- evaluation of overall residual risk acceptability (Clause 7);
- risk management report (Clause 8); and
- production and post-production information (Clause 9).

Figure 1 of ANSI/AAMI/ISO 14971:2007 (see Figure 1) provides a schematic representation of the risk management process. Central to the definition of risk are the concepts of probability of an occurrence of harm and the severity of that harm. Harm is defined in ANSI/AAMI/ISO 14971:2007 as "physical injury or damage to the health of people, or damage to property or the environment".

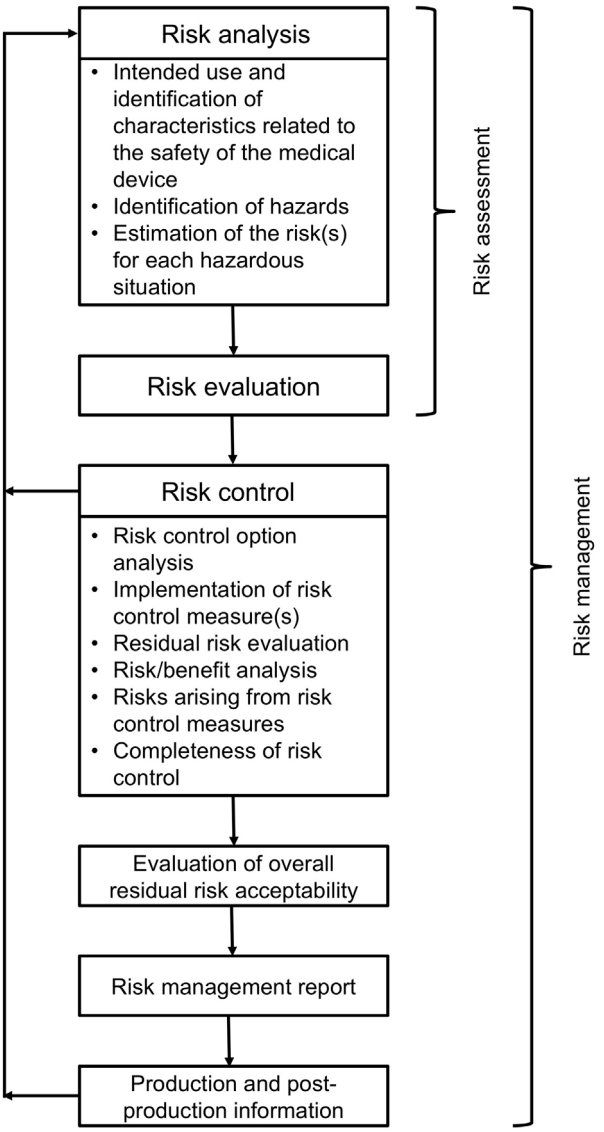

Figure 1 - Schematic representation of the risk management process (ANSI/AAMI/ISO 14971:2007)

The increased use of connected medical devices (i.e., devices directly connected to other systems or devices directly or via a computer network) has created a new source of risk for their safe operation. Security risks are associated with reduction of effectiveness and breach of data and systems security as included in the broader definition of harm in this document. While information security has been considered from the patient data privacy perspective for several years, there is no framework for security risk management for medical devices. This document describes a means of applying the risk management principles presented in ANSI/AAMI/ISO 14971 to the management of security risk.

The definition of harm is considered from the perspective of ANSI/AAMI/ISO 14971, as well as from healthcare information technology (IT) standards, such as the ANSI/AAMI/IEC 80001 family. Because a security risk management process that narrowly focuses on the traditional “physical injury or damage” definition may limit the scope of security risk mitigation, this document incorporates the broader considerations that risks include effects outside the traditional scope of patient physical harm and may include “reduction of effectiveness” and “breach of data and systems security” as extended in the ANSI/AAMI/IEC 80001 family of standards. Figure 2 shows the high-level relationship between these two classes of risk.

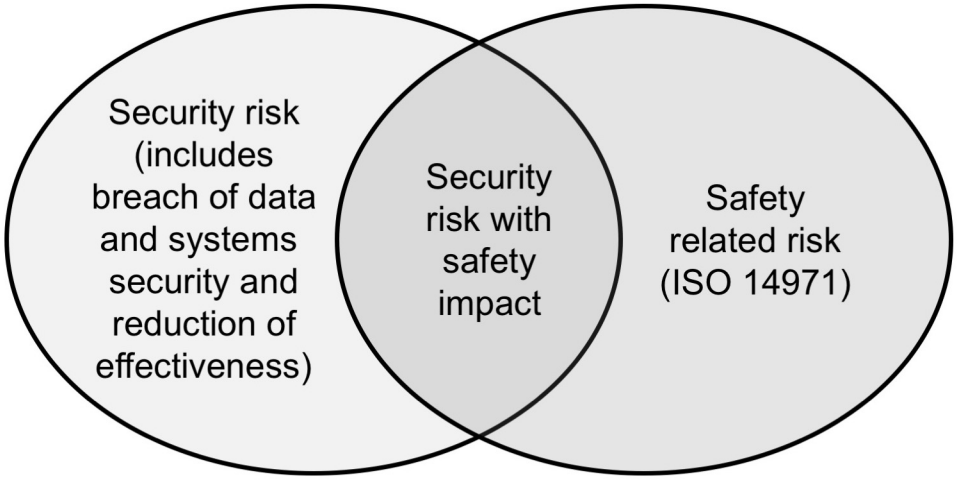

Figure 2 – A Venn diagram showing the relationship between security and safety risks

Considerations for security risk management are mapped to the risk management process steps of ANSI/AAMI/ISO 14971, as well as the security risk management process of NIST SP 800-30 Revision 1 *Guide for Conducting Risk Assessments (see Bibliography [53])*, with a particular emphasis on risk assessment methods. While this TIR utilizes NIST standards as a basis, manufacturers may use other generally accepted alternatives if they are better suited to their development processes.

Supporting annexes contain the following:

- Annex A: Security engineering principles and nomenclature – A high level overview of security engineering principles focused on their application to the medical device domain.
- Annex B: Security risk assessment – A more detailed description of the process for performing security risk assessment for a medical device based on the principles described in NIST SP 800-30 Revision 1 (see Bibliography [53]).
- Annex C: Generating cybersecurity requirements – A discussion on how to create effective, testable requirements for security properties that avoid complexities associated with “shall not” requirements. This is important since mitigating controls for security risks need to be expressed in the requirements for the device so proper verification of effectiveness can be shown.
- Annex D: Questions that can be used to identify medical device security characteristics – A detailed list of questions for manufacturers to assist in exploring security aspects of their devices, organized along the lines of ANSI/AAMI/ISO 80001-2-2:2010.
- Annex E: Security risk examples applied to medical products – A more detailed example of a fictional medical device and analysis of its security risks.
- Annex F: A comparison of terminology between key referenced standards – A comparison of the basic terms of risk management as defined in ANSI/AAMI/ISO 14971:2007, NIST SP 800-30 Revision 1, IEC 80001-1:2010 and this TIR.

While safety risk involves evaluating the probability and severity of a hazard leading to harm, security risk is based on an assessment of the likelihood that a threat will successfully exploit a device vulnerability, an event that could lead to an adverse impact due to a compromise of system confidentiality, integrity, and/or availability. This loosely parallels the concepts of probability and severity described in ANSI/AAMI/ISO 14971. Organizations should exercise caution when attempting to quantify likelihood of a future adverse impact in traditional probabilistic terms. Instead, they should focus on the skills and motivations of an attacker, and whether the effort required to exploit a vulnerability is less than the perceived gain the attacker will achieve by compromising the system (see B.2.1.1).

Security is an emergent property of a system. As such, the security of a device needs to be considered in the context of the broader system. This document directs manufacturers to understand, evaluate, and document the operating environment of a device so security risks are evaluated in their operational context. It is recognized that the manufacturer cannot ensure aspects of this operating environment that are outside the manufacturer’s control. However, it is incumbent on the manufacturer to understand the methods that Health Delivery Organizations (HDOs)

use to manage the risks of networked medical devices as specified in ANSI/AAMI/ISO 80001-1, as well as the methods used to communicate cybersecurity needs, risks, and controls as documented in ANSI/AAMI/ISO 80001-2-2. Manufacturers should understand the concept of a Responsibility Agreement[1] that may be negotiated with the purchasing HDO, and be prepared to communicate any specific security expectations of the network that the device is connected to through methods such as the HIMSS/NEMA Manufacturer Disclosure Statement for Medical Device Security (MDS2). Manufacturers should also recognize that a poorly secured and updated device could be a source of security vulnerability to other computing systems and other devices to which the device is connected, directly or on a shared network. Such a device can be used as a "pivot" to attack other systems and devices. A reasonable expectation of organizations deploying the device is that such risks have been considered and appropriately mitigated.

As a result, this document uses the broader definition of risk as used in the ANSI/AAMI/IEC 80001 family of standards. Manufacturers that follow the recommendations of this report should consider those risks that come from outside the device, mitigate those that are feasible, and document the expectations of the organization that becomes responsible for integrating the device into a broader network.

The framework described in this document is presented as a companion process to the safety risk management requirements of ANSI/AAMI/ISO 14971. This is similar to the risk management approach documented in ANSI/AAMI/IEC 62366-1:2015 for usability engineering. The key to successful integration of a device security risk management process into the larger risk management process is to bring together personnel with expertise in traditional device development, human factors, and cybersecurity product development. This collaboration will be essential to the ultimate goal of developing secure medical devices.

[1] Responsibility Agreements are described in ANSI/AAMI/ISO 80001-1.

Principles for medical device security – Risk management

1 Scope

This TIR provides guidance for addressing information security within the risk management framework defined by ANSI/AAMI/ISO 14971.

This guidance is intended to assist manufacturers and other users of the standard in the following:

- identifying threats, vulnerabilities, and assets associated with medical devices;
- estimating and evaluating associated security risks;
- controlling security risks; and
- monitoring effectiveness of the risk controls.

This document is based on an application of ANSI/AAMI/ISO 14971 with an expanded consideration of the possible impacts that a security compromise can have on the medical device, people, the environment, the manufacturer, and the information processed and stored by the device. This report also incorporates several principles from NIST SP 800-30 Revision 1 (see Bibliography [53]), a security risk management process developed for traditional IT systems.

The guidance provided by this document is applicable to all stages of the life-cycle of a medical device.

2 Terms and definitions

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

2.1
asset
person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value

[SOURCE: NICCS Glossary of Common Cybersecurity Terminology – As accessed on June 15, 2015.]

2.2
authentication
verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

[SOURCE: SP 800-53; SP 800-53A; SP 800-27; FIPS 200; SP 800-30]

2.3
authenticity
property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator (see Authentication)

[SOURCE: SP 800-53; SP 800-53A; CNSSI-4009; SP 800-39]

2.4
authorization
access privileges granted to a user, program, or process, or the act of granting those privileges

[SOURCE: CNSSI-4009]

2.5
availability
ensuring timely and reliable access to and use of information

NOTE 1 to entry: The phrase "use of information" encompasses delivery of intended functionality.

[SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542]

2.6
confidentiality
preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

[SOURCE: SP 800-53; SP 800-53A; SP 800-18; SP 800-27; SP 800-60; SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542]

2.7
data and systems security
operational state of a medical device in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

NOTE 1 to entry: Security, when mentioned in this document, should be taken to include data and systems security.

[SOURCE: ANSI/AAMI/IEC 80001-1:2010, 2.5, modified - "MEDICAL IT-NETWORK" has been replaced with "medical device" and Note 2 was redacted.]

2.8
effectiveness
ability to produce the intended result for the patient and the care provider

[SOURCE: ANSI/AAMI/IEC 80001-1:2010, 2.6, modified - "RESPONSIBLE ORGANIZATION" has been replaced with "care provider".]

2.9
emergency access
process or mechanism by which a device user can quickly and easily access the intended functionality in urgent (emergency) situations, bypassing the device's established access controls; the ability of the device user to access the indented functionality in case of an emergency situation that requires immediate access to the medical device

NOTE 1 to entry: Other access methods (e.g., "break glass") fall under this general definition but have varying levels of credentials and audit requirements.

[SOURCE: Adapted from HIMSS/NEMA Standard HN 1-2013 Manufacturer Disclosure Statement for Medical Device Security]

2.10
encryption
conversion of plaintext to ciphertext through the use of a cryptographic algorithm

[SOURCE: FIPS 185]

2.11
harm
physical injury or damage to the health of people, or damage to property or the environment, or reduction in effectiveness, or breach of data and systems security

[SOURCE: IEC 80001-1:2010, definition 2.8]

2.12
hazard
potential source of harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.5]

2.13
hazardous situation
circumstance in which people, property, or the environment are exposed to one or more hazard(s)

NOTE 1 to entry: See Annex E, ANSI/AAMI/ISO 14971:2007, for an explanation of the relationship between "hazard" and "hazardous situation".

[SOURCE: ISO/IEC Guide 51:1999, definition 3.6]

2.14
information security
protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

[SOURCE: SP 800-37; SP 800-53; SP 800-53A; SP 800-18; SP 800-60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542]

2.15
integrity
guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

NOTE 1 to entry: This definition includes therapy, device, and application integrity.

[SOURCE: SP 800-53; SP 800-53A; SP 800-18; SP 800-27; SP 800-37; SP 800-60; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542]

2.16
likelihood of occurrence
weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability

NOTE 1 to entry: Likelihood of occurrence combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).

[SOURCE: CNSSI-4009, modified - the phrase “In Information Assurance risk analysis,” was removed.]

2.17
non-repudiation
assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information

[SOURCE: CNSSI-4009; SP 800-60]

2.18
password
protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data

[SOURCE: CNSSI-4009]

2.19
personally identifiable information (PII)
any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

NOTE 1 to entry: Personally identifiable information is a superset of Protected Health Information (PHI).

[SOURCE: NIST SP 800-122; GAO Report 08-536]

2.20
predisposing condition
condition that exists within an organization, a mission/business process, enterprise architecture, or information system, including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, or other organizations

NOTE 1 to entry: Identical to NIST definition (SP 800-30 Revision 1) with the phrase “or the Nation” redacted.

[SOURCE: NIST SP 800-30 Revision 1]

2.21
residual risk
risk remaining after risk control measures have been taken

NOTE 1 to entry: Adapted from ISO/IEC Guide 51:1999, definition 3.9.

NOTE 2 to entry: ISO/IEC Guide 51:1999, definition 3.9 uses the term “protective measures” rather than “risk control measures.” However, in the context of this Technical Information Report, “protective measures” are only one option for controlling risk as described in 6.2.

2.22
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

2.23
risk analysis
systematic use of available information to identify hazards and to estimate the risk

NOTE 1 to entry: Risk analysis includes examination of different sequences of events that can produce hazardous situations and harm.

[SOURCE: ISO/IEC Guide 51:1999, definition 3.10]

2.24
risk assessment
overall process comprising a risk analysis and a risk evaluation

[SOURCE: ISO/IEC Guide 51:1999, definition 3.12]

2.25
risk control
process in which decisions are made and measures are implemented by which risks are reduced to, or maintained within, specified levels

[SOURCE: ANSI/AAMI/ISO 14971, definition 2.19]

2.26
risk evaluation
process of comparing the estimated risk against given risk criteria to determine the acceptability of the risk

[SOURCE: ANSI/AAMI/ISO 14971, definition 2.21]

2.27
safety
freedom from unacceptable risk

[SOURCE: ISO/IEC Guide 51:1999, definition 3.1]

2.28
threat
any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

NOTE 1 to entry: Identical to NIST definition (SP 800-53) with the phrase “or the Nation” redacted.

[SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009]

2.29
threat actor
individual, group, organization, or government that conducts or has the intent to conduct detrimental activities

NOTE 1 to entry: Synonymous with threat agent.

[SOURCE: NICCS Glossary of Common Cybersecurity Terminology – As accessed on June 15, 2015.]

2.30
threat analysis
examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment

[SOURCE: SP 800-27]

2.31
threat event
event or situation that has the potential for causing undesirable consequences or impact

[SOURCE: SP 800-30]

2.32
threat source
intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability

[SOURCE: FIPS 200; SP 800-53; SP 800-53A; SP 800-37]

2.33
top management
person or group of people who direct(s) and control(s) a manufacturer at the highest level

NOTE 1 to entry: Adapted from ISO 9000:2005, definition 3.2.7.

2.34
vulnerability
weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

[SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200]

3 General guidance for performing security risk management

3.1 Security risk management process

ANSI/AAMI/ISO 14971 requires that device manufacturers establish a risk management process for safety hazards to ensure that hazards are identified, risks are estimated, monitoring is established, and controls are put in place for those risks that require mitigation.

Security risk management should follow a similar path, as illustrated in Figure 3. While organizations may choose to incorporate security risks into their general safety risk management process, this document recommends the creation of a separate risk analysis process focused specifically on impacts that are identified by a security analysis. Because harm, as defined in this document, may include breach of data and system security and reduction in device effectiveness (as defined in ANSI/AAMI/IEC 80001-1), it is more appropriate to create a companion security risk management process to allow the organization to assess the additional risks associated with effectiveness and system/data security. If the processes are integrated, there could be an inclination to drop the evaluation of those risks that do not lead to harm as narrowly defined in ANSI/AAMI/ISO 14971, which can lead to incomplete or inconsistent security controls.

This segregation is further supported by the fact that security risk assessment models typically use assessment factors that are different from the model described by ANSI/AAMI/ISO 14971. In addition, integrating safety and security risk assessment into a single general risk management process may result in major modifications to a well-functioning safety risk management process.

Security risks that impact safety, according to the definition of harm in ANSI/AAMI/ISO 14971 (“physical injury or damage to the health of people, or damage to property or the environment”), should also be captured in the organization’s safety risk management process. It is recognized that treatment of risk in these two risk assessment models, safety risk assessment and security risk assessment, may differ. A specific risk assessed as “must mitigate” in one model might be assessed as “does not need further mitigation” in the other. Risk control measure(s) should be applied to bring the risk into the acceptable range in both assessment models.

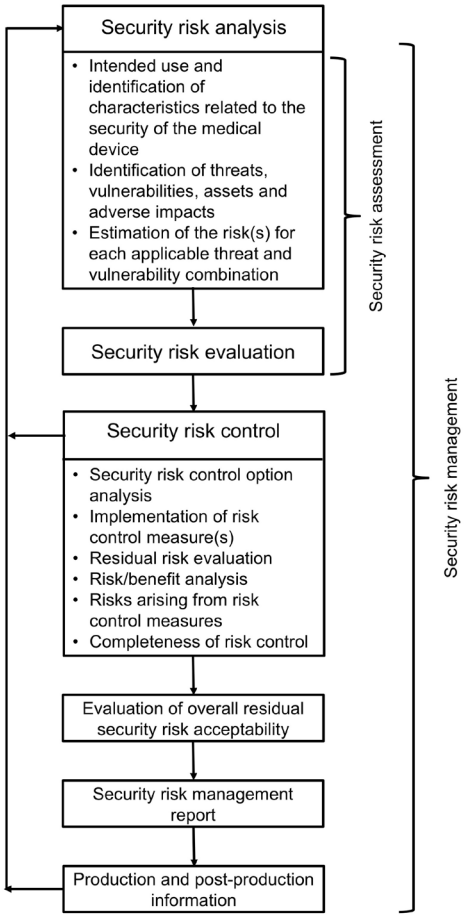

Figure 3 - Schematic representation of the security risk management process

3.1.1 Relationship between security and safety risk management

This document recommends that manufacturers establish a companion security risk management process to their existing ANSI/AAMI/ISO 14971-based safety risk management process. The requirements of ANSI/AAMI/ISO 14971 indicate that all hazards need to be managed through the safety risk management process – including those hazards that result from security compromises. However, because the definition of "harm" in this document is broader than the definition used in ANSI/AAMI/ISO 14971, there will be risks managed in the security risk assessment that are not propagated to the safety risk management process. An example would be a risk of compromise of the confidentiality of protected health information that is not considered harm in the context of ANSI/AAMI/ISO 14971, but clearly requires mitigation by the security risk management process. There are also business and reputation risks associated with a security compromise that are not considered harm in the safety sense.

When security risks may lead to safety risks, security and safety staff should work jointly to contribute to the security risk analysis and transfer safety related hazards to the safety analysis. An example of a security risk that is also a safety risk is a malicious attacker gaining access to a medical device's code, altering that code, and causing the device to malfunction. This malfunction may have the potential to cause harm to the patient. However, when a security risk does not involve safety risk, personnel qualified in security are typically sufficient for risk analysis. An example of a security risk that is not a safety risk is a malicious attacker who gains access to patient data. The patient data obtained poses a security risk but does not directly affect safety.

Because the security controls that mitigate safety risks caused by security compromise may simultaneously mitigate non-safety related security risks, it is logical to manage all security risks in a single process. That is, a security compromise that leads to harm (as more narrowly defined in ANSI/AAMI/ISO 14971) should be managed within the security risk management process and propagated for assessment using the organization's safety risk management process.

As illustrated in Figure 4, when a risk control measure is introduced to a design, the design must be reassessed to determine if the control measure introduces a new form of risk. It should be recognized that there is a coupling between safety and security risk assessment processes, so when control measures are introduced for one type of risk (e.g., safety), the manufacturer needs to assess the impact on the other type of risk (e.g., security) and vice versa. For example, the decision to add risk control measures for authentication might introduce risks that the device cannot be accessed in an emergency. The overall risk management process should identify those points of coupling and ensure that assessment of any newly identified source of risk is performed in both domains. This is illustrated in Figure 4, showing the logical connection points between the security and safety risk management processes.

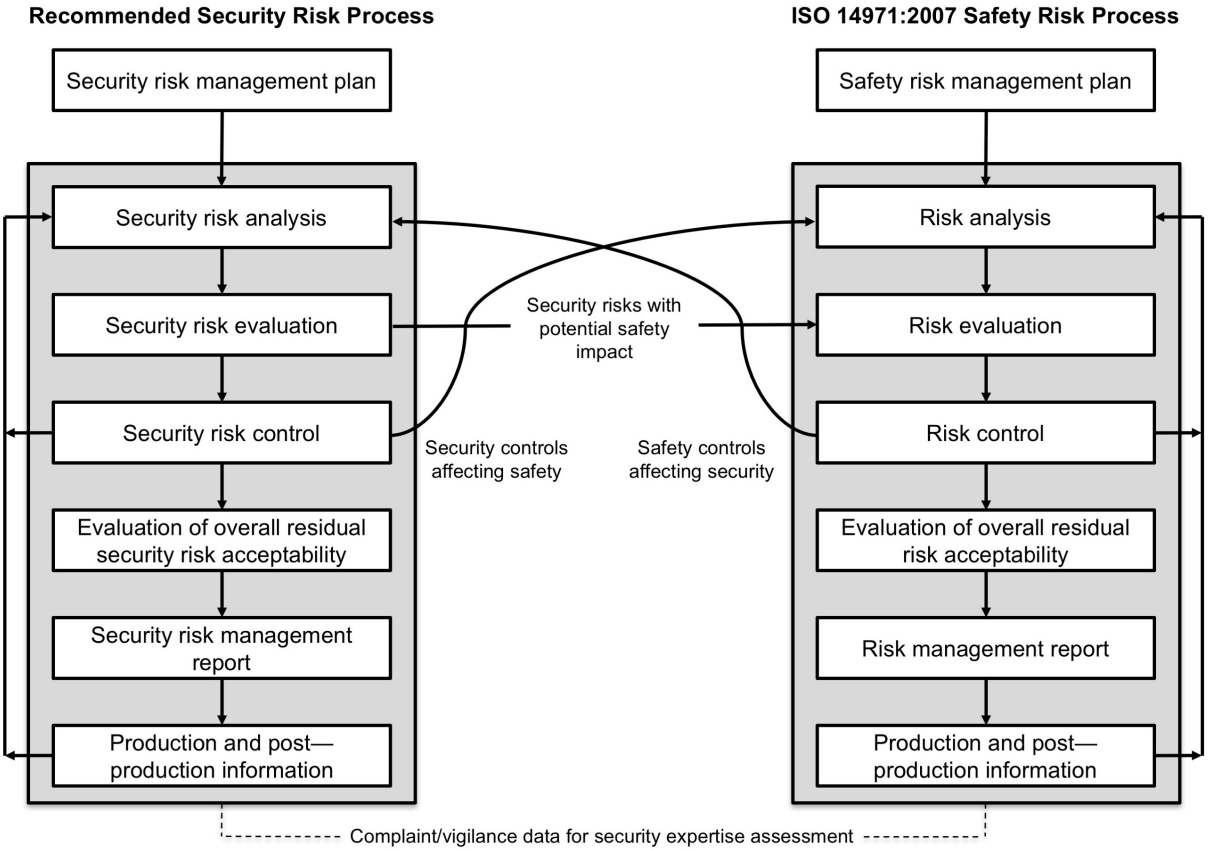

Figure 4 – Relationships between the security risk and safety risk management processes

Typically, these assessments iterate between the security and safety risk management processes. Figure 4 shows an example of one such iteration.

3.2 Management responsibilities

Top management should provide adequate and qualified personnel (see 3.3) to perform the security risk management process. In addition, top management needs to define and document the policy for determining the criteria for security risk acceptability, including criteria for non-safety related security risks, such as business and reputation risks. This policy should ensure that criteria are based upon applicable national or regional regulations and relevant international standards, and take into account available information, such as the generally accepted state of the art for security risk management and known stakeholder security concerns. Stakeholders include medical practitioners, Health Delivery Organizations (HDOs), governments, industry, patients, and members of the public.

Top management should ensure that the organization implements a coordinated vulnerability disclosure policy so security researchers and others have a means to communicate vulnerabilities identified in fielded devices.

Top management should review the suitability of the security risk management process at planned intervals to ensure the continuing effectiveness of the process, and they should document any decisions and actions taken.

3.3 Qualification of personnel

Persons performing security risk management tasks need to have the knowledge and experience appropriate to the tasks assigned to them. These should include knowledge of the particular medical device (or similar medical device) and its intended use, operating environments, security risk control technologies, and the risk management process.

Personnel should be knowledgeable in evaluating security threats and vulnerabilities, and be aware of past and emerging changes in the security risk landscape, both for medical devices, as well as general purpose computing systems. The team performing security risk management tasks should have experience with hardware and software architecture, design, and security test methods.

Appropriate qualification records should be maintained.

3.4 Security risk management plan

Security risk management should be incorporated into the manufacturer's risk management process. As discussed in 3.1, this document recommends that the security risk management process be maintained as a companion process to the safety risk management process. Because the two processes exchange information on the identified risks and candidate risk controls, the risk management plans for the two processes should be coordinated. However, it is acceptable for a manufacturer to incorporate the security risk management plan as part of the overall risk management plan developed in compliance with ISO 14971.

The scope of risk management activities includes the identification of the medical device features and life-cycle phases where security risks need to be managed. To properly determine the scope of security risk management activities, the medical device must be assessed to determine which features expose a potential security risk based on the intended use and operating environment. Because threats change over time and new vulnerabilities in operating systems, middleware and components are discovered on regular basis, security risks are frequently identified after a device is released to the market. Consequently, as threats evolve, it is critical to have a plan for post-market monitoring, reporting, analyzing, and responding to newly identified threats and vulnerabilities.

The criteria for risk evaluation, impact assessment, and residual risk acceptability should be documented in the plan. Because a vulnerability requires exploitation before harm can occur, there is a behavioral aspect to risk estimation that is not amenable to mathematical probability estimation. Because vulnerability requires exploitation before harm can occur, and exploitation involves human behavior, risk estimation is not amenable to mathematical probability estimation. Top management plays a critical role in defining a policy for determining the criteria for security risk acceptability (see 3.2).

The plan should describe the methodology for security risk verification. Some possible alternatives include the following:

a) verification testing of security controls that mitigate risks, including effectiveness of the mitigation;

b) robustness testing (e.g., "fuzz testing");

c) penetration testing (typically performed in a production equivalent or final configured state).

Manufacturers should also document any additional development methodologies that should be applied to reduce the likelihood of unintended functionality being present in the code that could become a vulnerability once deployed. This may include code analysis (e.g., inspections, static code checking) or particular verification testing strategies to increase confidence in the robustness of the implementation.

Consideration should be given to appropriate security testing for the intended use and operating environment (e.g., physical and network).

The security risk management plan should address how components (hardware and software) will be monitored for security performance and how vulnerabilities identified in those components are elevated for risk evaluation in the component's use in the finished medical device. Sources of information on new vulnerabilities for components include threat intelligence, reports from suppliers and the MITRE Common Vulnerabilities and Exposures (CVE) list. The plan should ensure that mechanisms for post-market cybersecurity surveillance of all third-party components will be identified.

The plan should describe how product security performance information will be collected in fielded devices and reported back to the manufacturer for assessment and potential control. The plan should reference the organization's coordinated vulnerability disclosure policy as an additional input source.

The security risk management plan should include the requirements for an appropriate review interval for newly identified threats and vulnerabilities.

NOTE See Clause 9 for additional guidance on recommended post-market surveillance activities and methods.

Manufacturers should plan for the appropriate disclosure of identified vulnerabilities.

Manufacturers should plan for a secure and efficient software update process to manage vulnerabilities in fielded devices and enable prompt response when required.

3.5 Security risk management file

The security risk management file may be integrated with the overall risk management file or be maintained separately.

The security risk management file should contain, at a minimum, the following:

a) security risk management plan;

b) security risk analysis components, such as:

   1) intended use and reasonably foreseeable misuse;

   2) qualitative and quantitative characteristics of the system that could affect the security of the medical device and, where appropriate, their defined limits; and

   3) risk controls and their implementation and verification;

c) security risk controls (typically captured and flowed down as system requirements specifications).

4 Security risk analysis

4.1 Security risk analysis process

Security risk analysis should be performed for the medical device as described in 4.2 to 4.4. The results of the security risk analysis should be recorded in the security risk management file.

Security needs to be assessed in the context of the larger system in which the device operates. The security risk analysis needs to consider the intended use and document the anticipated operating environment for which the device was designed and tested. The security architecture (see A.6) includes the complete operating environment of the device, as well as other important factors. These steps will facilitate communication to end user(s) responsible for device configuration.

If a security risk analysis, or other relevant information, is available for a similar medical device, then that analysis or information can be used as a starting point for the new analysis. The degree of relevance depends on the differences between the devices and whether these introduce new risks or significant vulnerability differences. The extent of reuse should be based on a systematic evaluation of the effects the changes have on exposing the patients, users, and manufacturer to additional risks.

In addition to the records recommended in 4.2 to 4.4, the documentation of the conduct and results of the security risk analysis should include at least the following:

a) a description and identification of the medical device that was analyzed;

b) identification of the person(s) and organization carrying out the security risk analysis; and

c) scope and date(s) of the security risk analysis.

4.2 Intended use and identification of characteristics related to the security of the medical device

For the particular medical device being considered, the manufacturer should document the intended use and reasonably foreseeable misuse. Reasonably foreseeable misuse should include efforts that normal users might make to circumvent security controls when they are perceived as preventing their use of the device.

NOTE 1 In this context, misuse is intended to mean incorrect or improper use of the medical device.

NOTE 2 The exploration of potential malicious abuse by attackers will be accomplished during the threat analysis activity documented in 4.3.

NOTE 3 Annex D contains questions that can serve as a useful guide in identifying medical device characteristics that could have an impact on security.

The manufacturer should document the assumed operating environment and security architecture for which the device is designed to operate, along with any assumptions on external security controls that must be provided by the end user. This documentation should be maintained in the security risk management file.

HDOs may have different and varying cybersecurity needs, risks and controls depending on the budget and sophistication of the organization. The manufacturer should perform a needs assessment with a representative sample of HDOs prior to initiating product design.

The manufacturer should document characteristics of the system that rely on user configuration to ensure the security of the device. The device's intended use and the experience level of the intended users should be understood to more accurately understand the likelihood of proper configuration by the end user.

The risk analysis should address characteristics of the device and its expected operating environment (physical and IT). For example, the risk analysis should consider whether the device is mobile and/or expected to be physically accessible to unauthorized users. Interoperability requirements and constraints of the operating environment should also be considered and documented. For medical devices that use wireless technology with a discovery mode or similar active connection mode, the manufacturer should implement appropriate technical controls to prevent unauthorized users from sensing or connecting to the medical device. In some cases, a manufacturer may document recommended compensating controls for implementation in the user environment.

4.3 Identification of threats, vulnerabilities, assets, and adverse impacts

In order to assess security risk, several factors need to be identified and documented.

The analysis of threats, vulnerabilities, assets, and adverse impacts can be performed in any order and may require participants with different skills and experiences. For example, understanding the adverse impacts may require members with deeper clinical understanding of the device's intended use, while the understanding of threats and their characteristics will require members with deeper security backgrounds.

This is expected to be an iterative process where continued brainstorming and discussion results in new aspects of the medical device being identified that could be affected by additional threats and vulnerabilities. The conclusion of the process is expected to provide a carefully considered and extensive listing of threats, vulnerabilities, and adverse impacts that feeds into the next step of estimating the risks.

NOTE See Annex B for examples of threats, vulnerabilities, assets, and adverse impacts.

4.3.1 Identification of threats

When assessing risk, special consideration should be given to threat actor capability and the benefits they might gain from a potential exploit. The risk analysis should document potential threats and the means a threat actor might use to exploit a vulnerability.

Threats can be identified using information from a variety of sources, including the manufacturer's IT security department, as well as from the security departments of key customers (e.g., large hospitals or clinics where the devices may be deployed). Information should also be gathered from reports of threats that have been experienced by the healthcare system, and from similar adjacent domains, such as industrial control systems. Governmental agencies, such as ICS-CERT, Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs), exist for the purpose of sharing this information. Information from third-party security information aggregators may also be helpful in gaining a thorough understanding of threat actors, their capabilities, and typical means of creating a threat event.

NOTE See Annex D and Annex E in NIST SP 800-30 Revision 1 (see Bibliography [53]) for additional material regarding threat identification.

4.3.2 Identification of vulnerabilities

The risk analysis should document known and potential vulnerabilities in the device. Vulnerabilities come from three distinct sources. First, vulnerabilities may be introduced by conscious design decisions, such as whether to include a security control or allow its bypass (e.g., in emergency access situations). The second source of vulnerabilities is from errors in the design, implementation, manufacture, or configuration of the device, by the manufacturer, their suppliers, or end users. These design errors are cases where the device does not meet the intent of the designers through a process deficiency. A third source of vulnerabilities is from a design characteristic that at the time of design release was not known to be a vulnerability, but subsequent to design release, a means of exploiting the design characteristic for malicious purposes was discovered. When assessing risk, special consideration should be given to the exploitability of the vulnerability (i.e., the capability necessary for a threat actor to exploit the vulnerability).

Vulnerabilities can be identified by incorporating top-down analysis methodologies (e.g. attack trees, threat modelling) to identify ways that a threat can cause loss of security properties for the device. Standards such as ANSI/AAMI/ISO

80001-2-2 list security capabilities, and this information can also identify potential vulnerabilities in the requirements. The identification process is best started early in the concept phase of the device development lifecycle but should also be applied to products in advanced stages of development or already in service.

Identification of possible points where a design/implementation error may introduce a vulnerability can be initiated with an analysis of the system to determine system nodes (components and users) and communication pathways. Once these are known for a system, they can be assessed for potential vulnerabilities that can affect each of these nodes and/or communication links. Various sources of information may also be used to identify vulnerabilities of the system under review. These sources include knowledge gained from past products, academic publications, industry news sources, independent security firms, independent research, and future projections. In addition, security testing (e.g., vulnerability scanning and penetration testing) may be used in early design phases to assist in identifying potential vulnerabilities. It is critical that the team performing the security risk assessment be knowledgeable on these and other pertinent sources of information so that a comprehensive and realistic identification of threats and vulnerabilities occurs.

NOTE See Annex F in NIST SP 800-30 Revision 1 (see Bibliography [53]) for additional material regarding vulnerabilities.

4.3.3 Identification of assets

Document the assets of the device. Assets can include information (e.g. patient data, diagnostic data, therapy parameters) the device itself, or components of the device including the device software. Assets may also be the physical interfaces to the device, in particular connections to external networks which could present risks to other systems on the network if unprotected at the device level.

Asset identification can be done through a systematic process, looking at each asset on the device and any interface that could be manipulated by an attacker. Asset identification should include those assets needed by the user to manage, diagnose, and treat the patient, as well as on those assets required to keep the device operating safely and securely. The process should consider assets needed to maintain the device or any used as part of post-market surveillance. Particular attention should be afforded to any stored authentication or cryptographic credentials that are used by the device, as their compromise could lead to the subsequent compromise of many other assets.

4.3.4 Identification of adverse impacts

For each identified asset, consider the impact that loss of confidentiality, loss of integrity, or loss of availability might have on safety, effectiveness, or data or system security.

Impact of asset compromise involves examining each asset and answering at least the following questions:

a) What is the impact if that asset's confidentiality was compromised, and the information it contained was available to an attacker?

b) What is the impact if that asset's integrity was compromised, and an attacker could change the information or software in a way that wasn't immediately obvious to the user (clinician or patient)?

c) What is the impact if that asset could be made unavailable?

d) Could the immediate impact of an asset compromise lead to another type of attack or vulnerability?

NOTE See Annex F in NIST SP 800-30 Revision 1 (see Bibliography [53]) for additional material regarding impact assessment.

4.4 Estimation of the risk(s) for each applicable threat and vulnerability combination

In the NIST SP800-30 Revision 1 model (see Bibliography [53]), security risk is estimated by a combination of the threat, vulnerability, and impact of asset compromise. When compared to the safety risk analysis process, the combination of threat and vulnerability is analogous to the probability of occurrence. The impact of asset compromise is analogous to the severity of harm.

The device manufacturer should establish a documented and repeatable risk estimation process that allows the security risk to be evaluated for acceptability. While the measures for the individual factors may be qualitative, it should be possible for subject matter experts to agree on the valuations of each factor, and the process by which they are combined results in a ranking of risk that can be used to decide which risks require further mitigation.

The outcome of this activity depends on the method employed by the manufacturer, but it is expected to be in the form of a ranking or grouping of the threats and vulnerabilities with possible additional details provided on rationale for the scoring.

NOTE See Annex G, H and I in NIST SP 800-30 Revision 1 (see Bibliography [53]) for additional material regarding risk estimation.

5 Security risk evaluation

Each identified risk needs to be evaluated for whether security risk reduction is required, according to the criteria documented in the security risk management plan. Each risk should also be evaluated to determine if a risk must be promoted to the safety risk file for analysis. As discussed in 3.1, security risks that can lead to hazardous situations need to be assessed in the safety risk analysis as well. The risk level should be mitigated (i.e., risk controlled) to an acceptable level in both analyses.

If reduction is determined to not be required, the manufacturer should document the rationale behind that decision and what changes in the threat environment would trigger reevaluation.

6 Risk control

6.1 Security risk reduction

Paralleling ANSI/AAMI/ISO 14971, when security risk reduction is required, the risk control activities in this clause should be performed.

6.2 Security risk control option analysis

Manufacturers should use a security risk control hierarchy that parallels the safety hierarchy presented in ANSI/AAMI/ISO 14971. Risk control options in order of preference are listed below:

a) Inherent security by design - Inherent security by design may include options, such as preventing access and/or modification of device settings from other systems or over the networked interface, implementation of secure certificates for authentication and code signing, incorporation of defense-in-depth, and various hardening mechanisms.

b) Protective measures in the medical device itself or in the manufacturing process - Examples of protective measures include requiring physical proximity, ensuring that malware detection is part of the software manufacturing and deployment process, and the addition of intrusion detection systems to detect attempted attacks.

c) Information for security - Information for security would include documenting security requirements that are placed on the entity or individual patient that connects the device directly to other systems or integrates the device on a network. Just as labeling for safety is considered a weak mitigation, leveraging excessive requirements on the network configuration to ensure security is least desirable, as one cannot be assured that all networks will be so configured, and it raises the potential that different devices on the same network are subject to incompatible requirements.

Manufacturers should be aware of the ANSI/AAMI/ISO 80001-1 concept of Responsibility Agreements and be prepared to supply the HIMSS/NEMA Manufacturer Disclosure Statement for Medical Device Security (MDS2) to those users of networked devices that request this document.

Manufacturers should consider the ability to respond to future unknown security risks as a key risk control measure, as there may be unknown vulnerabilities present in the designed medical device that become known as threats become more sophisticated. This includes the ability to securely deliver patches after the device is in service.

If, during risk control option analysis, the manufacturer determines the required security risk reduction is not practicable, the manufacturer should conduct a risk/benefit analysis of the residual risk (see 6.5).

6.3 Implementation of risk control measure(s)

The security risk control measures selected need to be implemented and verified with the results recorded in the security risk management file. These control measures will typically be expressed as testable requirements. Annex C provides guidance on documenting security requirements.

6.4 Residual risk evaluation

Residual risk is re-evaluated after the security risk controls have been applied. A risk control measure may mitigate either the threat, vulnerability, or impact. This should be documented to reflect the residual risk estimation. Further risk controls may need to be applied if the residual risk is unacceptable. Manufacturers need to determine what information about acceptable residual risks should be disclosed in the device labeling.

6.5 Risk/benefit analysis

Security risks that impact safety will need to be evaluated against the manufacturer's acceptability criteria for their safety risk management process per ANSI/AAMI/ISO 14971. For security risks that do not impact safety, the decision not to mitigate may be more appropriately rationalized with a cost/benefit analysis.

If security residual risk is considered unacceptable, a risk/benefit analysis should be performed. The manufacturer should appropriately balance the residual security risk against the benefit that might be gained by the design capability or security control. For example, a conditionally unacceptable risk of exposure of personally identifiable information (PII) [74] should not be deemed acceptable, because the device delivers life-saving therapy. In this example the benefit of having PII stored in the device should be compared to the risk of confidentiality loss.

If analysis determined that the security risks are outweighed by the benefits, the manufacturer should determine what information should be communicated in the device labeling to manage this residual risk. This needs to be communicated in such a way that it does not provide a blueprint for a potential attacker to exploit the non-mitigated vulnerability.

NOTE "Security by obscurity" is not considered a valid risk reduction method. Undisclosed vulnerabilities may ultimately be discovered, which could result in elevated risk (due to increased likelihood of exploit) forcing corrective action post-deployment, if the manufacturer becomes aware of the discovery. Because there is always the potential that the discovery can be hidden from the manufacturer, unmitigated vulnerabilities that have high adverse impact carry significant residual risk.

6.6 Risks arising from risk control measures

The manufacturer should seek to balance usability, device safety, and device security to ensure that the security controls are appropriate for the intended users and any systems to which the device is connected. Related decisions and trade-offs should be documented. It is possible that new risks of harm could be unintentionally added to the system due to the implementation of security controls (e.g., use of password authentication which adds unacceptable delay in accessing the device during an emergency). Each proposed security risk control should be analyzed for the potential of introducing new safety and security risks.

The manufacturer should consider whether there could be impacts on patient compliance and device effectiveness due to changes in device usability. Utilizing human factors experts in this process remains an important and critical part of a balanced assessment.

6.7 Completeness of risk control

Manufacturers should ensure that the risk(s) from all identified threats, vulnerabilities, and potentially compromised assets have been considered and the implemented controls are comprehensive in addressing them. Record the results in the security risk management file.

A security controls assessment should be performed, based on a security control set derived from customer requirements, regional compliance expectations, and industry best practices. From the security control set, appropriate security controls can be selected based on device functionality and operating environment. The selected controls can then be evaluated to determine whether they are sufficient. Missing security controls may indicate vulnerabilities and threats not previously considered, resulting in a return to the security risk analysis step (see 4.1).

A security controls assessment can also be performed as part of security risk analysis. This would create an additional mechanism for the discovery of vulnerabilities earlier in the assessment process.

7 Evaluation of overall residual security risk acceptability

Clause 7 of ANSI/AAMI/ISO 14971:2007 requires that the overall residual risk be evaluated against the criteria stated in the risk management plan. Just as there are complexities in evaluating the overall residual safety risk (see Clause 6 in ANSI/AAMI/ISO TIR 24971:2013), determining overall residual security risk is difficult. The impacts of various potential security exploits vary according to different severities, and the means to estimate how likely it is that a threat actor will exploit a vulnerability and cause adverse impact can be variable as well.

Another complexity is that the overall residual risk acceptability may vary by the nature of the adverse impact. A manufacturer may choose to establish overall residual risk criteria that address different acceptable overall residual risk levels for direct physical harm (i.e., causing harm to the patient that is due to interaction with the device) versus loss of effectiveness versus loss of data or systems security. Generally accepted security practices should be considered as part of the residual risk acceptability decision-making process.

The manufacturer should employ security testing (e.g., vulnerability scanning and penetration testing) as a means to aid in the assessment of overall residual security risk. However, it should be noted that such negative testing is

minimally conclusive. Passing a penetration test does not indicate that a device is invulnerable, but that it resisted the forms of attacks represented by that specific penetration test suite at that specific test date.

For an overall residual risk that is judged acceptable, the manufacturer should decide which documentation regarding information security is necessary to include in the accompanying documents in order to manage the overall residual risk.

8 Security risk management report

A security risk management report summarizes the evaluation, assessment, mitigation activities, and traceability to the verification reports of security controls that ensure a device is reasonably secure. This report should provide references to the detailed plans and reports for readers seeking additional information. The report should be periodically updated as new threats, vulnerabilities, assets, or adverse impacts are discovered, and as post-market information becomes available.

At a minimum, the security risk management report should provide, either directly or by reference, the following items:

a) Risk analysis, mitigations, and design considerations pertaining to cybersecurity risks. Consider including the following:

   1) system description including intended use;

   2) description of the operating environment;

   3) assets;

   4) vulnerabilities;

   5) impact of asset compromise; and

   6) security risk controls.

b) A traceability matrix of security risks to security controls.

c) Traceability to the verification reports for documented security controls.

d) A description of when and how security updates/patches will be provided.

e) A description of the steps taken to assure devices will be delivered malware-free.

Prior to release for commercial distribution of the medical device, the manufacturer should carry out a review of the security risk management process. This review should assure at least the following:

— The security risk management plan has been appropriately implemented.

— The overall residual security risk is acceptable.

— Appropriate methods are in place to obtain relevant production and post-production security information.

9 Production and post-production information

Manufacturers should be monitoring, collecting, and reviewing information about the operating environment for the medical device during production and post-production phases. Monitoring should include the time period from when the medical device is submitted for regulatory approval and before the product is released.

During the production phase, manufacturers should be monitoring that devices are being produced in a manner that avoids the introduction of unintended functionality (e.g., malware) into the device that could affect the performance of the device, or serve as a threat to other devices to which it may be connected in the operating environment.

During the post-production phase, manufacturers should have in place means to monitor whether fielded devices are being exposed to security threats and whether the implemented security controls are effective in mitigating those threats. This is typically done through the creation of a security log that is secured from tampering. The manufacturer should consider the mechanisms used by the operator, end user, or those responsible for installation, use, and maintenance of the device for collecting, processing, and communicating this monitoring data.

The manufacturer should also monitor security information from the supply chain providing hardware and software components for the medical device. A means should also be established to accept reporting of potential device

vulnerabilities from non-indicated users (e.g., security researchers) and to monitor reports of identified vulnerabilities in similar devices from the same or other manufacturers.

The collected information should be evaluated for possible relevance to device security and possible impacts on patient harm, with particular focus on the following:

- emergence of new classes of threats;
- identification of previously unrecognized vulnerabilities, or new methods of exploiting existing vulnerabilities; and
- a change in the previously estimated risk level for a known vulnerability.

If any of these conditions occur, the impact on the previously implemented risk management activities should be evaluated and a review of the risk management file for the medical device should be conducted. The manufacturer should also evaluate if there is a change in the assessed residual risk and the acceptability of that residual risk. These results should be recorded in the risk management file.

Because the threat environment can change without specific new events being captured by surveillance mechanisms, manufacturers should plan for a periodic review of the security of their medical device as documented in the security risk management plan.

Manufacturers should also ensure that they maintain the capability to respond to security issues for the expected life of the fielded devices. This capability could include software patches available for download to mitigate vulnerabilities discovered during post market surveillance activities.

Vulnerabilities identified by or reported to a medical device manufacturer should be disclosed to appropriate stakeholders within a reasonable timeframe as established by the organization's coordinated vulnerability disclosure policy. These disclosures are not restricted to vulnerabilities which have an identified patch or field change. Expedited disclosure may be needed to facilitate control of unacceptable security risk.

Annex A
(informative)

Security engineering principles and nomenclature

A.1 Overview

Good system engineering practices should be applied to security engineering. They represent a robust approach to the design, creation, and operation of systems and include these steps:

- identification and quantification of system goals;
- creation of alternative system design concepts;
- evaluation of design trade-offs;
- selection and implementation of the best design;
- verification that the design is properly built and integrated; and
- post-implementation assessment of how well the system meets (or met) the goals

The complexity of medical device systems and the security risks from unintended emergent system behaviors requires the use of good system engineering practices throughout the product lifecycle.

Medical devices present unique and challenging demands and constraints on the security architecture. Most of the differentiating characteristics between conventional IT and a medical device arise because medical devices require the following:

- risk benefit analysis and the context of use;
- focus on hazard analysis;
- testing that focuses on minimizing risk of injury or damage; and
- clinical implications of security-sensitive software updates

These constraints often impact security attributes and create unique challenges as outlined in Table A.1.

Table A.1 – Examples of security attributes and comparison between conventional IT and a medical device

Security Attribute	Conventional IT	Medical Device
Access	No access without credential	Emergency access possible without credentials
Access management	Centralized	Localized to patient
Accessibility	Typically accessible	Intermittent accessibility and may be inaccessible
Product lifecycle	Constant flow of new and revised products	Device or platform used for decades
Computing resources	Vast and expandable	Sometimes limited and/or severely power-constrained
Updates and monitoring	Continuous connectivity and less likely to require end-to-end validation	More likely to require end-to-end validation
Consequences	Economic	Safety

A.2 Uniqueness of embedded medical systems

Embedded systems are typically resource constrained, yet must satisfy manufacturing cost, development cost, reliability, power, safety, and security requirements. Although many embedded systems are non-standard or proprietary, they are not innately secure.

There are a variety of possible attacks on embedded systems. Different defenses are needed when the attacker has physical access to the system. With physical access, the attacker is no longer restricted to using communication ports. It may be necessary to provide hardware security in the form of conformal coatings, blind and buried traces, non-heat-sensitive glue, and other techniques that force the attacker to damage the product if they attempt to reverse engineer the design. Tamper-evident seals are useful for attacks against individual devices that may be left in place after modification.

A number of techniques may be used to increase the difficulty of reverse engineering and exploitation of an embedded system, such as the following:

- disabling unused communication interfaces;
- limiting physical access to communication interfaces;
- activating security fuses or other protection mechanisms;
- proper use of firmware encryption; and
- disabling unused firmware components.

Embedded system security considerations should be taken into account early in the design process and throughout the product development lifecycle.

A.3 Stakeholders

Stakeholders have a valid interest in the system and may be affected by it either directly or indirectly. Stakeholders often include:

- anyone who operates the system;
- anyone who benefits from the system;
- anyone involved in maintenance of the system;
- anyone involved in administration of the system;
- anyone involved in purchasing or procuring the system;
- organizations that regulate aspects of the system; and
- organizations responsible for systems that interface with the system.

A.3.1 Patients, family, friends, and caregivers

Patients benefit directly from the therapy or diagnostic information the devices provide. They want their therapy to improve their quality of life without adding stress or fear from the potential risk of a security-related event. Also, there are trends toward increased patient engagement in their care that can cause the inclusion of new features with potential security impacts. For home-based medical devices, there may be others (e.g., caregivers) who support the patient and work with the medical device.

A.3.2 Regulators

Regulatory agencies wish to protect the common good of those they serve. They are less concerned with the survival of a business than with the effectiveness and safety of the medical therapies.

A.3.3 Health Delivery Organizations (HDOs)

HDOs look for the most effective methods to provide care for their patients. Systems with lower cost and lower risk are more attractive. An increased security burden and related events may decrease the attractiveness of a system.

A.3.4 Manufacturers

Manufacturers take into account business constraints while addressing the needs of patients and customers. Security can create additional burden and expense. Excessive burden can turn away customers and make systems overly cumbersome and expensive. The business desires effective security solutions that enhance product value in excess of its cost.

A.3.5 Academics

Academia seeks to learn and publish new information. Their goal may be to influence regulation, obtain research funding, or employment.

A.3.6 Cyber Liability Insurers

Cyber liability insurance companies are beginning to better quantify cybersecurity risks and will likely drive economic incentives to improve cybersecurity when there is potential for financial loss.

A.4 Security objectives and goals

The overarching goals of a safety risk process are safety, effectiveness, and maintaining essential performance (as defined by ANSI/AAMI ES60601-1:2005/(R)2012) of the medical device. Security adds the following additional primary objectives:

- confidentiality;
- integrity (includes authenticity and non-repudiation);
- availability.

The preceding primary security objectives may be further broken down into more specific sub-objectives:

- ensuring that data is not improperly altered;
- ensuring alarm limits are not altered where alteration may make the device unsafe;
- ensuring the identity of authorized user is known so important actions may be logged and attributable to a user (accountability)—in some cases this objective may be partially achieved through physical access controls;
- ensuring the integrity of audit security audit logs to prevent tampering.

Annex D contains a set of questions that can be used to help define the requirements for medical device security architecture.

Basic security objectives can be met only when the design addresses a comprehensive set of use scenarios that include abuse cases, misuse, system constraints, the needs of all stakeholders, and the operating environment. The manufacturer should also recognize that the threat landscape is constantly evolving and establish processes for monitoring and performing periodic review of the security architecture to assure it continues to be effective.

A.5 Considerations for emergency access

Emergency device access may mean HDOs need to have access without a prior relationship with the patient or the medical device. The attending physician or health care professional expects to obtain immediate access to the medical device in an emergency scenario. Specific techniques for emergency access include location-controlled access, limited communications capability in an emergency mode, access logging, secondary communications protocols for emergency access, and proximal communications techniques (i.e., very short-range - e.g., centimeters). Proximal communications is one way of establishing trust, because it is common medical practice and it allows the patient to be engaged in the trust-establishment procedure. Therefore, it may be acceptable for communication systems using proximal techniques to rely on physical security in a limited-access operating environment (e.g., temporarily disabling mechanisms for confidentiality and authentication). Positive initiation of emergency access and subsequent logging of the event are important to deter abuse.

A.6 Medical device security architecture considerations

A security architecture should include categorized assets, security controls, threat agents, major functional blocks, communications paths and protocols, trust zones or chokepoints, data flows, and interactions with external systems.

Components of a security architecture should include but are not limited to, the following:

- Actors – individuals or systems that interact with the data, protected data, and security controls, their capabilities, needs, limitations, constraints, etc.;
- Data – the information that passes through the security model, whether protected or not, whether at rest or in motion;
- Data protection mechanisms – access control and integrity protection;
- Hardware security blocks – trusted hardware, function, and limitations;
- Untrusted hardware – any hardware to which an attacker is likely to gain access;
- Trusted software/firmware;
- Untrusted software/firmware;
- Data use – how data is used. (e.g., user workflows, use scenarios);
- Patient – the recipient of medical care;
- Location – location of where a particular medical device is intended to be used – for example, whether

hospital-based or mobile (as with an implantable device); and

— Other assets that need to be secured.

These entities are expressed in architectural views that are selected to best communicate the architecture. Possible views include the following:

— architectural overview;

— physical;

— functional;

— information;

— concurrency;

— software implementation;

— process;

— sequential;

— logical;

— technology;

— deployment; and

— operational.

Many manufacturers create their own systems consisting of several devices that evolve on separate timelines. There are unique architecture considerations in this situation. A new product added to an existing system can have a positive or negative impact. The new product can impact both the device manufacturer and the healthcare delivery organization. Potential impacts include the following:

— Enhancement: A new product feature may enhance the security architecture by taking advantage of unused capability (e.g., the system supports signed firmware updates, present products do not, but the new product does).

— Planning: A new feature may position a new product to take advantage of security architecture growth (e.g., the new product can use signed messages for remote programming, but the system does not yet support the feature).

— Reduction in security: The new product may negatively impact the current security architecture if it does not support a security architecture feature (e.g., the security architecture and existing products supports encrypted communications but the new product does not as documented in FIPS 140-2).

— Neglect: The new product may negatively impact future security growth (e.g., the future security architecture will include security logging, but the new device does not support the capability).

Security assessments on products consider not only the present state, but also address the projected future state of the complete system. A platform that does not allow for incremental improvement as new products are released will not be viewed as favorably as one that does accommodate security improvements.

It is important that the security architecture be broad and open-ended. Not all future added components need to be understood today, but it is important to know that the security architecture will support growth towards the desired future state.

Annex B
(informative)

Security risk assessment

As discussed in Clause 4, security risk management requires the identification, analysis and evaluation of all potential security risks, so appropriate design decisions can be made on which risks require mitigating controls, and which risks can be accepted and monitored for changes that may require re-assessment. This annex provides supporting detail on assessment techniques that may be applied to perform the steps of security risk analysis and evaluation.

No single security risk assessment methodology is applicable to all medical device manufacturers without tailoring, but all good methodologies must do the following:

- provide a consistent means to assess and reason about security risk across the organization;
- avoid assessment factors that rely on “gut judgment” in favor of those that can be evaluated dispassionately;
- allow the organization to clearly rank risks and identify those that are acceptable, conditionally acceptable, and unacceptable; and
- enable comparison between “traditional” safety risks and the risks associated with a security vulnerability so that the organization can apply resources to mitigate the overall highest set of risks. Security controls implemented after this comparison should be verifiable.

While there are several security risk assessment processes available, most of them have been developed for IT systems, including web-based services. The most commonly used process is the one documented in NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments (see Bibliography [53])*. Indeed, many of the other published assessment processes can be mapped to the NIST standard. This TIR follows the basic outline of that NIST standard, with specific emphasis on how it should be connected to the 14971-based safety risk management process required for medical devices. Manufacturers who are developing an internal security risk management process are encouraged to read NIST SP 800-30 Revision 1 (see Bibliography [53]) thoroughly, as it contains many useful recommendations that are not replicated here. In addition, the manufacturer should consult applicable regulatory guidance such as the FDA’s *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (see Bibliography [17]) when defining their security risk assessment activities.

Manufacturers should define a security risk assessment methodology consisting of these four steps:

a) Define the risk assessment process to be used, including the steps.

b) Define an explicit risk model, including which risk factors will be assessed and the relationships between risk factors.

c) Define the assessment approach (quantitative, qualitative, or semi-qualitative), ranges of values, and how they can be combined to evaluate risk.

d) Define the analysis approach (e.g., threat-oriented, asset/impact-oriented, or vulnerability-oriented), describing how combinations of risk factors are identified/analyzed to ensure adequate coverage of the problem space at a consistent level of detail.

The clauses of this Annex provide guidance in the development of an assessment methodology, and how security risk is evaluated.

B.1 Risk assessment process

A high-level assessment process is shown in Figure B.1.

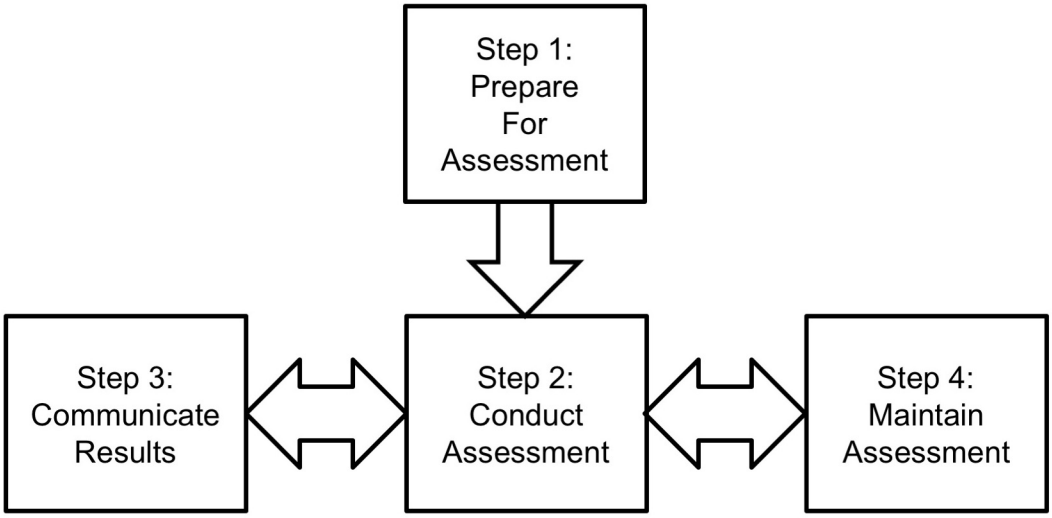

Figure B.1 - A basic high-level risk assessment process[2]

Four primary activities should be implemented in the manufacturer's security risk management processes and are outlined in B.1.1 through B.1.4.

B.1.1 Prepare for assessment

As part of the overall security risk management plan, the manufacturer should document the following items regarding the security risk assessment step.

a) Identify the purpose of the assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support. Define the specific linkages between security risk assessment and safety risk assessment as discussed in Clause 3.

b) Identify the scope of the assessment, including the following:

   1) The operating environment and how it is managed when the device is in use.

   2) The breadth of the device lifecycle to be covered: including design, test, manufacturing, deployment, field updates, refurbishment/repair, and retirement.

c) Identify the assumptions and constraints associated with the assessment, including the following:

   1) Types and granularity of threat sources and threat events that should be considered.

   2) Types of vulnerabilities to be considered and the process to be used to identify potential vulnerabilities.

   3) The range of operating environments to be considered for the device being assessed.

   4) The level of acceptable risk tolerance and uncertainty may also be documented.

d) Identify sources for threats, vulnerabilities, and impact to be used in the risk assessment.

e) Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

   1) Identify the processes to combine assessment factors into estimates of likelihood, impact, and risk.

   2) Identify the assessment approach to be used (quantitative, semi-quantitative, or qualitative. See B.3).

   3) Identify the analysis approach to be used (threat-oriented, asset/impact-oriented, or vulnerability-oriented. See B.4)

[2] Adapted from Figure 5, NIST SP 800-30 Revision 1 (see Bibliography [53])

The results of these decisions should be documented and provided to the assessment team.

B.1.2 Conduct assessment

The activities associated with conducting a security risk assessment are documented in B.2 through B.4.

B.1.3 Communicate results

The manufacturer should define the form and frequency of information to be communicated to organizational decision makers. This can be in the form of briefings, summary reports, information dashboards, or other communication vehicles that are consistent with how safety risk assessments are delivered.

Of specific importance is defining the communications mechanisms to pass information between the security risk assessment and safety risk assessment teams. Key members of each team should participate in the assessment activities of the other team.

B.1.4 Maintain assessment

Security risk assessment maintenance is done throughout the product lifecycle, even during product development, as new information from outside the organization may indicate updates to risk assessments are required. Such information might be the identification of new threats that are focusing attention on Health IT and medical device networks, new threat events impacting health or related industries, or new vulnerabilities identified in software components that are incorporated into the device in development (e.g., operating system or third party code libraries).

Maintenance should also be planned during the supported life of the device, similarly focusing on learned changes to the threat landscape that could impact the risk assessment and require reassessment of potential mitigating controls or software updates.

B.1.5 Other security risk assessment processes

While this guidance focuses on the NIST assessment process, there are other models that may be appropriate, depending on the device and organizational development processes. The following subclauses document a few options.

B.1.5.1 Common vulnerability scoring system (CVSS)

CVSS is an open industry standard for assessing the severity of computer system security vulnerabilities, maintained by the Forum of Incident Response and Security Teams (FIRST). The US National Vulnerability Database uses CVSS scoring to rank critical vulnerabilities.

CVSS requires the assessment/scoring of several metrics for each assessed vulnerability. These metrics are combined using a formula specific to the CVSS model into scores for “Exploitability” (or likelihood) and “Impact.”

B.1.5.2 Open web application security project (OWASP)

OWASP is a “worldwide not-for-profit charitable organization focused on improving the security of software.” The OWASP Risk Rating Methodology creates a risk assessment measure through evaluating Likelihood and Impact. Like the NIST and CVSS models, a set of discrete measures is assessed, and the model computes the Likelihood, Impact, and overall risk for a vulnerability.

B.1.5.3 Attack trees

Attack trees are a technique that can be used in security risk assessments to assess the risk of a security violation from one of many possible attacks or from a combination of attacks [12][20][67].

Attack trees are similar to fault trees used in Fault Tree Analysis (FTA). As in FTA a parent node may require one of many (OR) or a combination (AND) of successful attacks for a security violation represented by the parent to be considered successful. Unlike FTA, however, attack trees are not derived from random statistical events and are therefore not amenable to quantitative determination of probabilities using Bayesian statistical methods.

Attack trees use a holistic approach to security, including not only components and subsystems, but larger system attributes, such as human interaction, servers, and networks. Analysis of attack trees can identify not only technical defects in a system, but also weaknesses in physical security procedures and operating procedures. Attack trees recognize that it is almost impossible to eliminate all defects in components, but that a secure architecture will limit and lessen the consequences of these failures. Attack trees combine the knowledge of subject matter experts from diverse fields, including human factors, into a single model that provides a high-level picture of security.

Attack tree models show if an adversary is capable of performing a specific attack and which attacks are most desirable to attackers. The combination of feasibility and desirability provide an indication of the likelihood of specific attacks by a given adversary. The consequence of the attack on the victim can be incorporated into the model to assess risks associated with various attacks.

B.2 Risk model

As stated in NIST SP 800-30 Revision 1 (see Bibliography [53]), "*Risk models* define the *risk factors* to be assessed and the relationships among those factors." Typical risk factors that make up a model are shown in Figure B.2, including threats, vulnerabilities and impacts. Threats can be evaluated for intent (or goals) and capabilities. Vulnerabilities may either pre-exist in the design/implementation (inherent) or may be introduced by the threat as a means to exploit the device (e.g., when malicious software is introduced into a system to create a new vulnerability).

Impacts may either be reversible (e.g., when known good copies of information are restored from a backup) or may be irreversible. This later case covers impacts that cross over into device safety – for example, if a device is tampered with to change therapy settings or make it non-functional when it is needed in a critical situation.

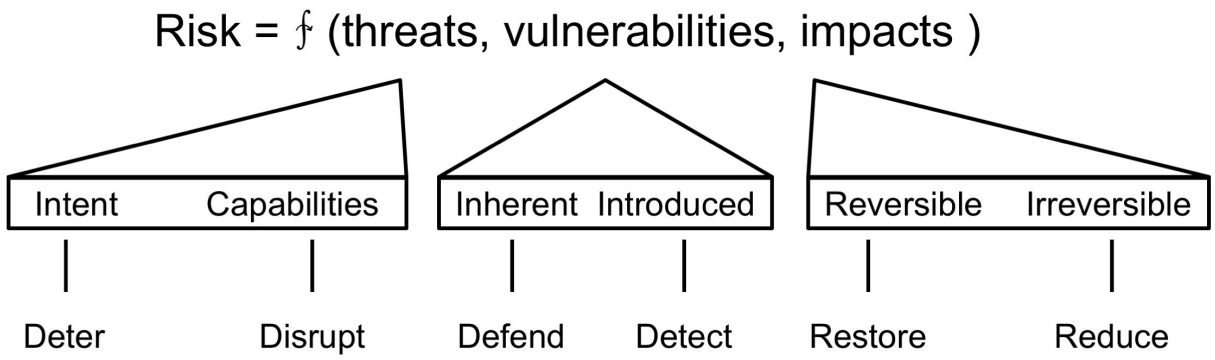

Figure B.2 - Security risk is assessed using three primary factors[3]

As illustrated in Figure B.2, security risk is a function of the three primary factors – threats, vulnerabilities, and resulting impacts. Security controls can be implemented to reduce the effect of any of the risk factors. Some of the methods are listed at the bottom of Figure B.2.

A generic process for risk assessment is shown in Figure B.3. The process begins by an assessment of the risk factors–threats, vulnerabilities and impacts. The order in which these are assessed can vary depending on the organization, the assessment goals, the device, and its intended use. A discussion of the alternatives can be found in B.4.

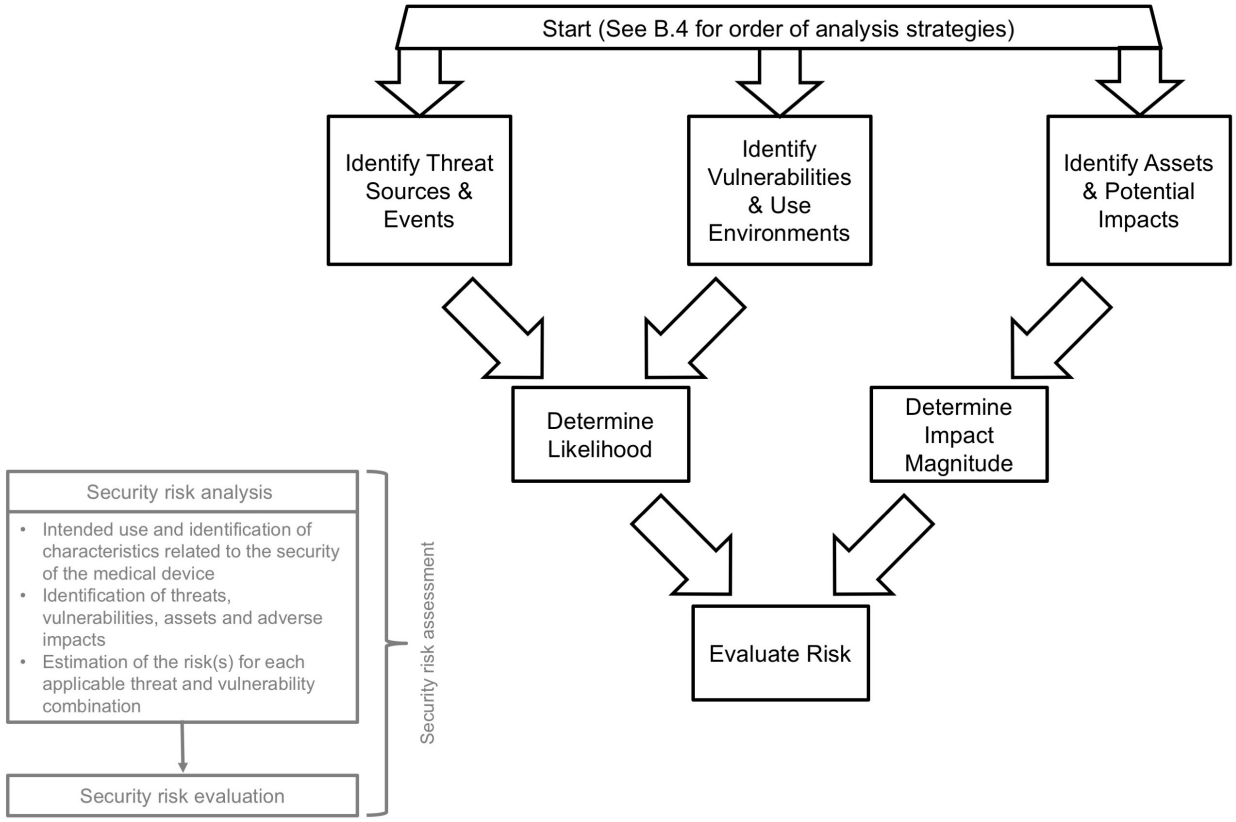

Figure B.3 - Security risk assessment process[4]

[3] Adapted from *Resilient Military Systems and the Advanced Cyber Threat* - Defense Science Board (see Bibliography [19])

The following subclauses address the assessment of the three main risk factors.

B.2.1 Threat assessment

Threat sources may be adversarial or non-adversarial. One class of non-adversarial threats comes from user error, and the processes followed to meet ANSI/AAMI/IEC 62366-1 medical device usability requirements should include risks associated with use and misuse of the security features of the device. Manufacturers should consider both the normal use of the device, as well as the steps required to securely set up the device, and to maintain it. For example, if user confusion causes poor maintenance of a secure device, security properties may be lost.

Depending on the characteristics of the device being assessed, non-adversarial threats from natural events such as weather may also be appropriate to consider. If the device function requires interaction with a high-availability remote computing function (such as a cloud service), then such natural events could impact the availability of that service, and it should be included in the security risk assessment process.

Manufacturers should document potential adversarial threats from malicious actors as one of the critical security risk factors. These threats should go well beyond those threats that may already have been experienced by the manufacturer, as the threat landscape is constantly changing, and the attacks experienced in the past are very poor indicators for what may be attempted in the future. This is a fundamentally different approach from that used by safety risk assessment methods where historical data on failure rates can be a good metric for predicting similar failures in the future.

When appropriate for the type of device, robust intrusion detection and security logging methods should be designed into a remote monitoring system to ensure that this data will have predictive value.

Understanding the range of possible threat actors and the methods they may use to attack a device requires a thorough understanding of the nature of these attacks on other systems, and vigilance on the constantly changing capabilities and tools they use.

B.2.1.1 Characteristics of adversarial threats

In most cases, adversarial threat actors are rational human beings who have technical capabilities that they use to try to achieve their goals. Understanding these patterns can help the manufacturer identify what group(s) and method(s) are most likely to be used in an attack against a medical device.

Manufacturers should also recognize that there are three broad reasons why their device may be subject to an attack:

a) An attacker is creating general purpose malware to harvest computing to achieve other purposes, such as creating a botnet, sending spam or mining bitcoins (to name a few reasons). Manufacturers who use common COTS operating systems and tools may be at risk to such malware, even though it is not specifically targeted to their device.

b) The attacker may wish to exploit assets via other vulnerable connected devices or through the network that the device is connected to (such as PII or insurance information), and they use the device as a “pivot” to gain access to the network or other computing equipment. The general knowledge that medical devices are slow to be patched, and often are based on old, vulnerable software versions can make them attractive targets for well-established attack vectors.

c) The attacker specifically targets the medical device, either to gain access to information contained in the device, or to interfere with the device’s operation.

Manufacturers have traditionally only considered the latter category to be their responsibility, and may dismiss it as unlikely. However, the joint responsibility of the end user and manufacturer to ensure that the health delivery system is safe and secure makes all three categories relevant when understanding the potential threats.

A study commissioned by the Department of Defense, *Resilient Military Systems and the Advanced Cyber Threat* - Defense Science Board (see Bibliography [19]), noted that different classes of threats have significantly different technical capabilities and resources. The report categorized “threat tiers” as shown in Figure B.4 and Table B.1.

While the assessment of risk will ultimately define the degree of required security controls, it is recommended that medical device systems that include a risk of injury include an analysis and associated defenses for threat tiers I through IV.

[4] Adapted from NIST SP 800-30 Revision 1 (see Bibliography [53])

Threat assessments need to be maintained, as the threat landscape is changing quickly. The recent past has demonstrated an increasingly short time between an exploit being developed by one of the higher-capability threats (such as a nation-state) and its repurposing and use by one of the lower capability attackers (such as organized crime). The short time between the disclosure of the Heartbleed vulnerability in 2014 and its use to attack health care systems (on the order of 1 month) is evidence of the rapid adoption of new knowledge by attackers to achieve their goals.

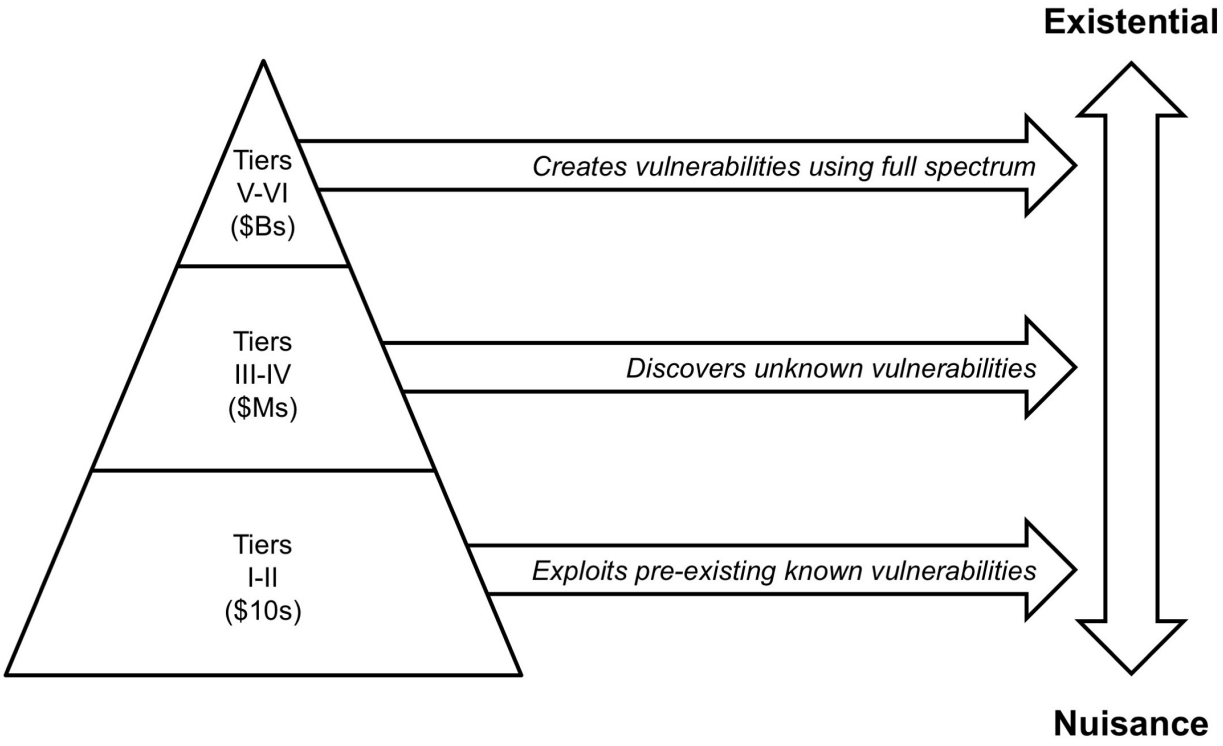

Figure B.4 - Cyber Threat Taxonomy[5]

For each threat source, analyze and document the following characteristics:

- Skill level – As captured in the threat tiers, different attacker classes have different capabilities. When combined with vulnerabilities (see B.3), a determination can be made of which attacker class may have the technical capabilities to mount a more complex exploit.
- Motivation – Attackers have a wide range of motivations that can include fame, financial gain, intellectual property, curiosity, anger, or even having a political agenda.
- Desire for anonymity – Some attackers require anonymity to consider their attack a success, and may only mount their attack from a remote location. Other attacker classes seek personal attention and may attack a sample device as a "demonstration" to embarrass the manufacturer and obtain fame.

[5] From Figure 2.1 in Resilient Military Systems and the Advanced Cyber Threat - Defense Science Board (see Bibliography [19])

Table B.1 - Description of Threat Tiers6

Tier	Description
I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publicly known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode rootkits, frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to "influence" commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.

B.2.1.2 Threat events

Threat events are the means by which a threat actor mounts an attack. Enumerating potential threat events helps the manufacturer understand the various methods attackers might use to get into their device and focus efforts on developing lists of potential vulnerabilities that might make the attacker successful.

To develop a comprehensive list of threat events the risk analyst should examine the techniques that a malicious actor might follow. In other words, "think like a hacker". Some of the steps attackers use to penetrate a system are listed below:

- Reconnaissance - collecting intelligence about the system;
- Penetration - gaining access to the system;
- Enumeration - discovering other system resources; reconnaissance from within the system;
- Execution - conducting a computer network attack or computer network exploitation;
- Maintenance - maintaining access to the system by importing tools and installing backdoors; and
- Concealment - obfuscating to prevent discovery of the exploit or the access tools.

Appendix E of NIST SP 800-30 Revision 1 (see Bibliography [53]) contains a list of potential threat events organized along similar categories. Another useful source of threat event information is the Common Attack Pattern Enumeration and Classification (CAPEC) list maintained by MITRE and the US Department of Homeland Security (see Bibliography [46]).

[6] From Table 2.1 in Resilient Military Systems and the Advanced Cyber Threat - Defense Science Board, January 2013

B.2.1.3 Example threats

The following list can be used to aid in the identification of possible threats and their potential motivations. This list should not be considered comprehensive, and the manufacturer should assemble one that is tailored to the specific characteristics of their device and its deployment into use in the field. Manufacturers should use threat source data from NIST, the Health IT sector, and from related business sectors (such as Industrial Control Systems) to create a comprehensive, up-to-date list.

a) Adversarial Actors

   1) Nation States (Tiers IV-VI)

   2) Organized Crime (Tier IV)

   3) Disgruntled/ex-employees (Tier II-III)

   4) Political Activists (Tier I-III)

   5) Emotionally unstable (Tier I-III)

   6) “Script kiddies” (Tier I)

b) Non-adversarial Actors

   1) Academic researchers (Tier II-III)

   2) Professional security researchers (Tier II-III)

   3) Unintentional Misuse

      i) Inexperienced users

      ii) Inexperienced installers

      iii) Inexperienced maintainers

c) Other threat sources

   1) Natural events

   2) Integration effects, such as

      i) RF Interference

      ii) Incompatible software

      iii) “Misbehaving” third party systems on network

      iv) Vulnerable systems or devices directly connected to the device (e.g., via RS-232, USB, or other “hardwired” non-network connections)

B.2.2 Vulnerability assessment

While some of the more notable vulnerabilities that have been reported are weaknesses in implementation, or “bugs” (e.g., Heartbleed, Shellshock, etc.), others can be due to design decisions, or problems in how a device is used in the field. For example, the decision to use a common, fixed password for the maintenance account on all devices from a manufacturer is a design choice that creates a vulnerability that can be easily exploited if that password becomes generally known.

A thorough vulnerability assessment is a critical component to a comprehensive security risk assessment, as it is impossible for an organization to make good decisions about which vulnerabilities need to be mitigated if it is unaware that they are present.

Identifying potential vulnerabilities can be done in several ways. First, there are common catalogs of known vulnerabilities in existing, fielded systems. One of the largest is the Common Vulnerabilities and Exposures List maintained by MITRE under funding from the United States – Computer Emergency Readiness Team (US-CERT) (see Bibliography [46]). The US-CERT also maintains a set of publications and vulnerability alert notification tools to allow manufacturers to keep in touch with changes and trends.

Manufacturers should also be aware of the various Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs), including the National Health ISAC (NH-ISAC) that covers the healthcare sector. ISACs and ISAOs are used for information sharing regarding cybersecurity incidents and can be a source of information about vulnerabilities that are being exploited in existing systems.

Manufacturers should also utilize published information to avoid introducing common errors into their own software that might become a vulnerability. The IEEE Center for Secure design has a published Avoiding the Top 10 Software Security Design Flaws (see Bibliography [37]). MITRE also supports a Common Weakness Enumeration (CWE) list (see Bibliography [48]) that provides a unified, measurable set of software weaknesses that is a useful reference as well.

Manufacturers are also encouraged to become familiar with the tools used by the attacker community – often the same tools that are used by third party "penetration testers" to determine if a system is resilient to a wide variety of known attacks. One of the most common is the open source tool, "Metasploit."

Commercial off-the-shelf (COTS) subcomponents are another source of system vulnerabilities that are often overlooked or assumed to be secure. COTS subcomponents include hardware devices, software modules developed by other organizations, and the operating system (OS). Some OSs, first designed for desktop or general purpose computing, enable many interfaces by default through network connections, wireless and other interface ports. Manufacturers should analyze the OS to identify enabled communication features that are not used directly by the device software, as these provide ingress for threat vectors.

Additional sources of system vulnerabilities are those discovered during post-launch monitoring. Vulnerabilities discovered post-launch present a high risk, because fielded devices may not be updated until the patient returns for a checkup or the device receives periodic maintenance or service update.

Predisposing conditions can include aspects of the operating environment. For example, a device that is only used within an operating room might depend on the physical security of the hospital to ensure that only authorized users physically interact with it. Predisposing conditions may be assessed for their pervasiveness in order to determine to what extent a vulnerability may be mitigated by them. If that same device is also used in outpatient clinics or locations where physical security cannot be assured, the vulnerabilities exposed by the physical user interface may be of greater concern in the overall risk assessment.

B.2.2.1 Example vulnerability classes

The following list can be used as a starting point to aid in the identification of vulnerabilities that may be exploited by a threat. It should not be considered a complete set, but should be expanded as appropriate.

a) Physical environment of the system
    1) Information displayed on a screen
    2) Physical security
    3) Power availability
b) Personnel
    1) Users
    2) Developers
    3) Support staff
c) Management
d) Administrative procedures and security measures within the organization
e) Business operation and service delivery
f) Hardware
    1) Debug interfaces enabled
    2) Use of removable media
    3) Lack of physical tamper detection and response
g) Software

1) Memory safety violations
2) Input validation error
3) Race conditions
4) Privilege-confusion
5) User interface failures

h) Communication equipment and facilities
1) Side channels

B.2.3 Impact assessment

The third risk factor that needs to be assessed is the possible impacts that a threat source could cause if an attack is successful. This will be broader than the set of harms that are considered in the safety risk assessment, as it should include factors such as information loss, loss of trust/reputation, as well as loss of device effectiveness.

The following list is an adaptation of the impact examples in Appendix H of NIST SP 800-30 Revision 1 (see Bibliography [53]). It can be a starting point for medical device manufacturers in developing an organization-specific impact list that can help with the identification of applicable harm(s):

a) Impact to Operations
1) Loss of device effectiveness
2) Loss of device therapy
3) Loss of availability

b) Impact to Assets
1) Physical
2) Information
3) Communications

c) Impact to Individuals
1) Physical injury or loss of life
2) Inappropriate or suboptimal therapy
3) Loss of PII
4) Patient concern

d) Impact to other organizations or the environment
1) Damage to property
2) Damage to the environment
3) Device becomes vector to attack other systems

It is also appropriate for a manufacturer to consider the business impact of cybersecurity breaches, which are completely separate from any harmful degradation of the device's intended use or effectiveness. A data breach, for example, might lead to penalties for disclosure of PII, and the financial impact of such a data breach should be a factor in security mitigation decisions, whether that impact is to the manufacturer or to their customer (which would result in a loss of trust and reputation for the manufacturer).

B.2.3.1 Asset inventory

One of the useful tools in creating a comprehensive list of potential impacts is to first document a complete set of device assets. Once complete, for each asset, consider the impact if the asset had a loss of confidentiality, integrity, or availability. The importance of these factors will vary depending upon the specific device involved. For example, a device that does not store or communicate patient identifiable information may meet its intended use with little

concern for confidentiality, so vulnerabilities that degrade confidentiality may be of less concern than those that degrade integrity. Similarly, a device that provides therapy may have a very high requirement for integrity and availability.

Another factor to consider in completing the asset inventory is to identify any asset that would be an attractive target for an attacker. Based on the attacker motivations discussed in B.2.1, there may be specific device assets that would help an attacker achieve their motivations. For devices that may be connected to a broader network (e.g. HDO intranet) the attractive target may be the information in systems on that network, and the threat actor may want to use vulnerabilities in the device to conduct such an attack, with undetermined impacts on the device's operation.

The following list can be used as a starting point to aid in the identification of the assets that may be the target of value for a threat. It should not be considered a complete list, but should be expanded as appropriate.

B.2.3.2 Asset identification

Physical Assets

a) User interface
b) Device assets
    1) Operating system
    2) Software libraries
    3) Application software
    4) Keys/Certificates
    5) Device identity
    6) Device resources
        i) Processing
        ii) Memory
        iii) I/O
    7) Physical interfaces
c) Device telemetry
d) Network interface

Information Assets

a) Patient data
b) HDO data
c) Insurance/coverage data
d) Device settings/programming commands
e) Passwords
f) Configurations
    1) Network
    2) Infrastructure
g) Diagnostic logs
h) Physical location
i) Telemetry data
j) Session credentials (keys, tokens, etc.)

B.3 Assessment approaches

The safety risk assessment approaches presented in Annex D of ANSI/AAMI/ISO 14971 include quantitative, semi-quantitative, and qualitative examples. Many assessment models for traditional safety risk management encourage the use of quantitative measures, and statistics collected from past device performance can be a rich source of data to calibrate such models. However, security risks that result from a vulnerability being intentionally exploited by some threat actor involves human behavior. As a result, most security risk assessment models use qualitative or semi-quantitative measures to assess risk.

Qualitative approaches typically use a small set of non-numeric values (e.g., Low, Medium, High) and can be quite subjective unless clear definitions are provided for how these values should be chosen. Semi-quantitative approaches that use a set of bins with numeric ranges may allow the risk assessment team to use subject matter experts (or small set of them) to agree on the assignment of values, allowing more reasoning about the values, while still allowing mapping to a set of qualitative values when the final recommendations are reported out to management.

Regardless of which approach is selected, the manufacturer should clearly document the decision criteria and how the resulting assessment values for the different risk factors are agreed upon.

B.4 Security analysis approaches

As was shown in Figure B.3, the three risk factors (threats, vulnerabilities, and impacts) are interrelated in that knowledge of one of the factors may assist in determining what to analyze for the other factors. There are three different approaches that can be used, depending on which risk factor is assessed first:

- Threat-oriented – First identify the threat sources and events, through the development of threat scenarios. Identify the vulnerabilities that are likely to be exploitable by those threats and impacts based on the threat actor's motivations. (See Figure B.5).

- Asset/impact-oriented – Perform a complete asset inventory and assess the potential impact if those assets are compromised. Identify vulnerabilities that could lead to those impacts and threat sources/events that might initiate exploits utilizing those vulnerabilities. (See Figure B.6)

- Vulnerability-oriented – Begin by analyzing potential vulnerabilities and pre-disposing conditions that may be exploitable. Identify threat events and sources that could initiate those exploits, and then capture the potential impact if the exploits were successful. (See Figure B.7)

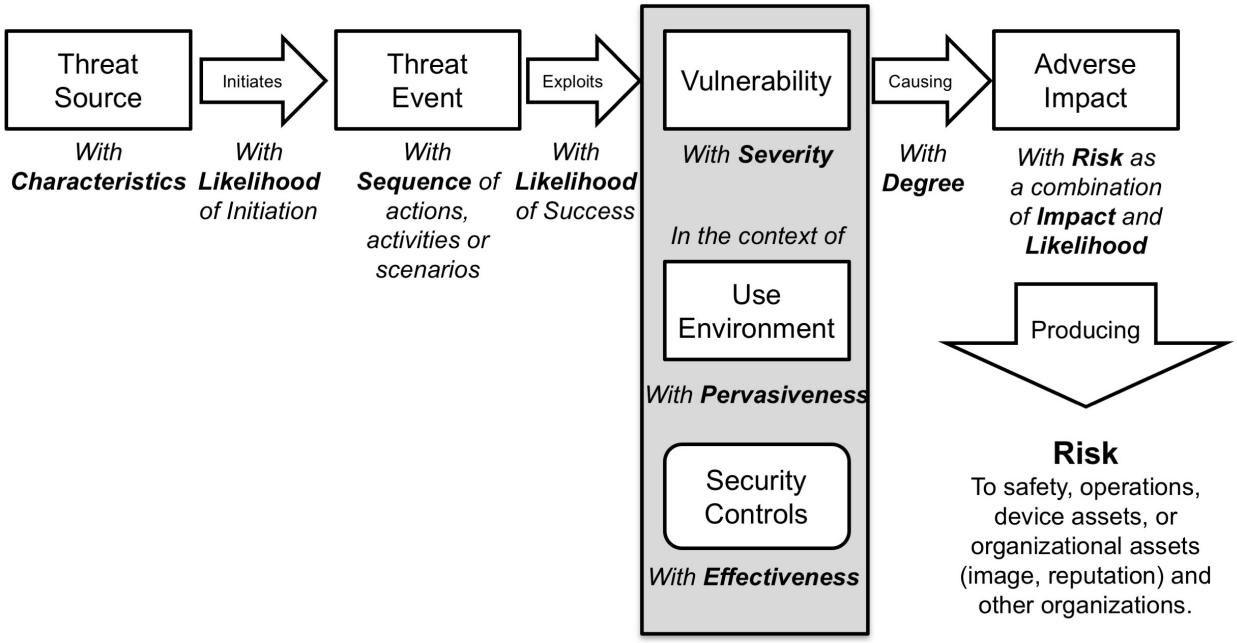

Figure B.5 - An example Threat-oriented Security Risk assessment approach[7]

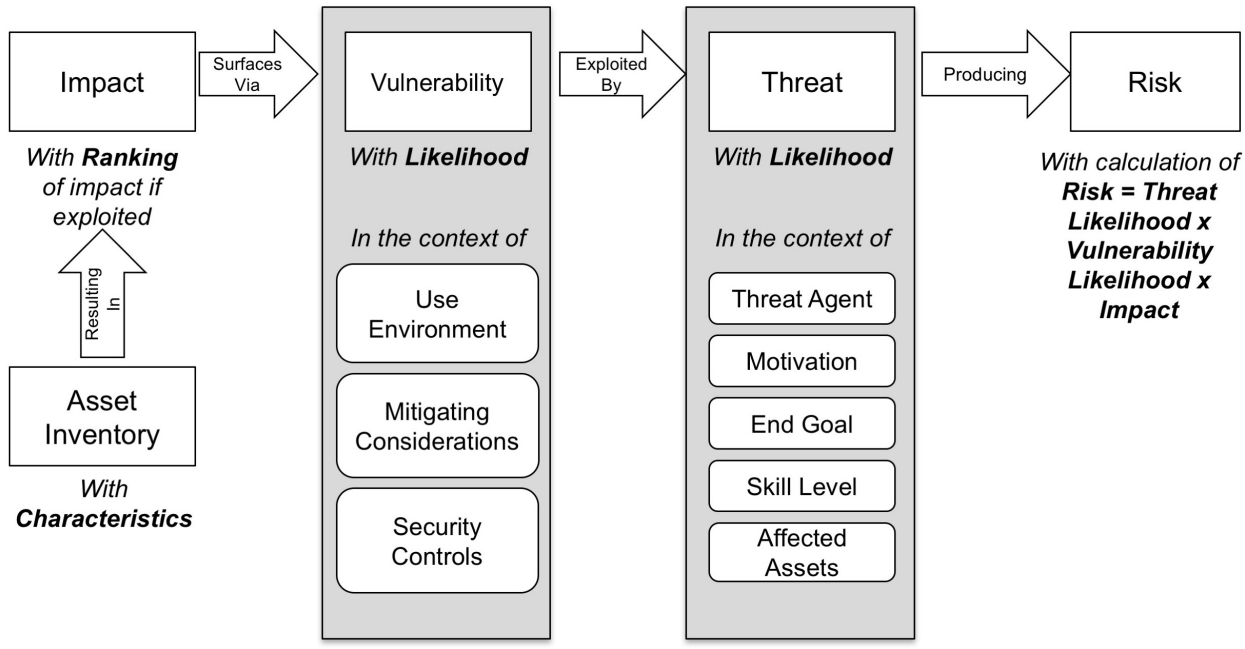

Figure B.6 - An example Asset-oriented Security Risk assessment approach

[7] Adapted from NIST SP 800-30 Revision 1 (see Bibliography [53])

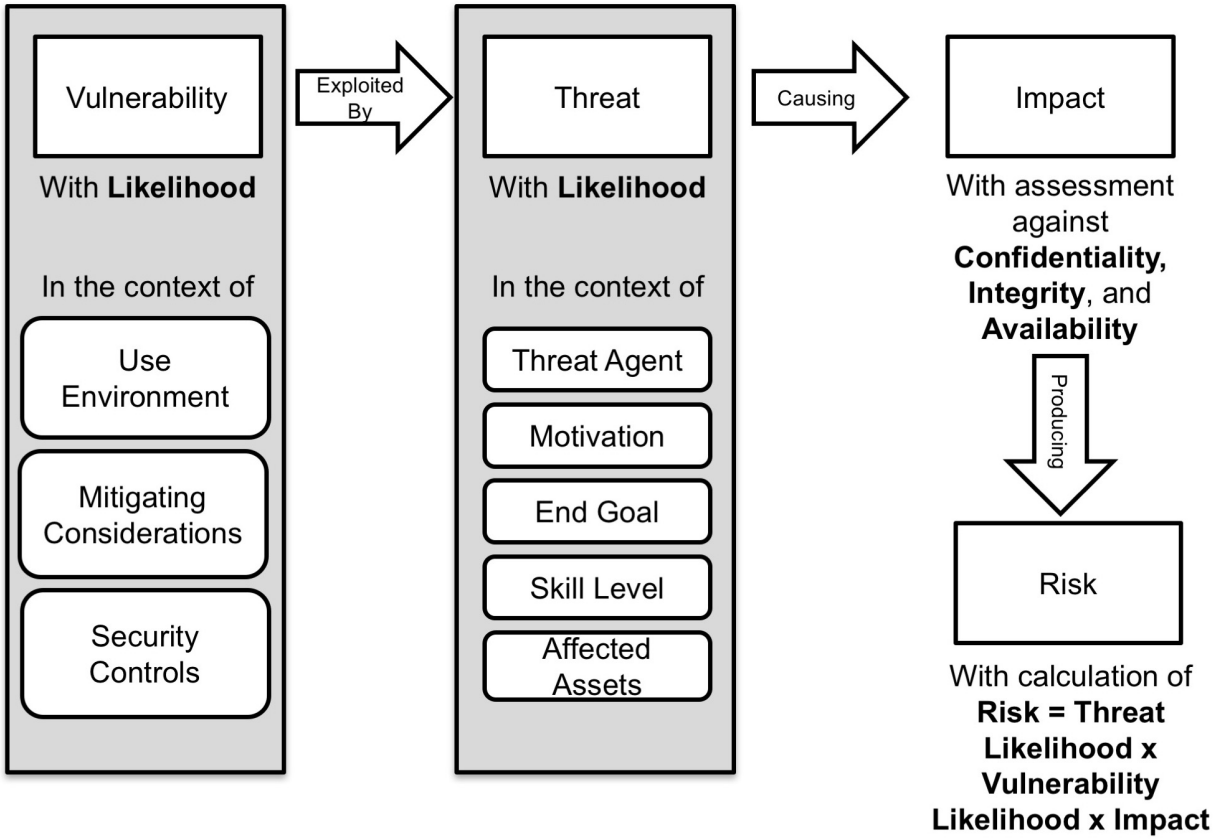

Figure B.7 - An example Vulnerability-oriented Security Risk assessment approach

The choice of which approach to follow is up to the manufacturer and should be documented in the security risk management plan. Choices should be driven by knowledge of the organization and goals of the risk analysis. If the target of the analysis is a complete system or if there are specific threats that need to be addressed, a threat-oriented approach may be appropriate. If it is a single device that will be used in the context of a larger system by an end-customer, an asset/impact-oriented approach may be the best. It is also useful to consider multiple approaches, as the biases built in to one approach may cause some risks to be missed. A second approach may also be used by an independent "red-team" that can be used to look for critical risks that may have been missed.

During post-market deployment, new risks may be learned through the exposure of new vulnerabilities. A vulnerability-oriented analysis approach is likely the most appropriate to respond quickly when needing to determine if a risk mitigation is required when the vulnerability is discovered.

B.5 Assessing security risk

Security risk is assessed by combining the likelihood that a threat will successfully exploit a vulnerability and result in an impact with the severity of that impact.

Safety risk is defined as the "combination of the probability of occurrence of harm [to the patient, other user or environment] and the severity of that harm." Traditional safety risk management approaches were designed to deal with random failures in which the likelihood of occurrence is largely based on design and manufacturing factors. In such cases, probability is often a statistical estimate, or the multiplication of a set of independent probabilities to predict future occurrence.

In contrast, in security risk assessment likelihood is an estimate of whether an attacker will invest the time and resources to exploit that vulnerability to achieve something the attacker sees as valuable. While human motivations are not amenable to traditional statistical analysis, a likelihood is typically assessed by combining the assessments of a threat and a specific vulnerability. The manufacturer's overall risk model should define the specific factors and how

they are combined to produce a qualitative or semi-quantitative likelihood value. Caution should be applied, as factors may not be independent.

The resulting likelihood value for an exploited vulnerability can be combined with the impact of the exploit to determine an overall security risk level. Organizations should define the levels of acceptable, conditionally-acceptable and unacceptable risk. Security risk controls should be implemented to reduce the risk to an acceptable zone. These controls should also be assessed to determine if they result in a new safety or security risk.

Annex C
(informative)

Generating cybersecurity requirements

The backbone to security risk management is the ability to express the medical device security behaviors, including mitigations and risk controls, in the form of verifiable requirements.

Cybersecurity requirements are implemented to reduce the security risks by decreasing the likelihood that the device's confidentiality, integrity, and/or availability are intentionally or unintentionally compromised. The cybersecurity requirements generation process starts by the identification of security controls through the security risk assessment techniques described in Annex B. The identified security controls are then used to draft verifiable security requirements that reside within the design history file for the medical device.

The generation of security requirements should follow system engineering best practices. Each individual requirement should be:

- Attainable: Technically and legally possible;
- Unambiguous: Simple, concise, standalone expression of a whole idea or statement;
- Clear: Not confusing, using simple words, concise statements, and consistent language;
- Consistent: Not in conflict with other requirements;
- Verifiable: Can be determined that the system meets the requirement either via verification or validation;
- Necessary: Essential to meet the need of a stakeholder by implementing a security control;
- Design free: Does not specify a design approach; and
- Positive: Written in the affirmative, not the negative.

To generate good security requirements, the following questions should be asked:

- Is this security requirement technically and legally possible?
- Can the intended audience describe the security constraint on the device from this requirement?
- Can the intended audience identify the subject of the requirement (e.g., component, system, interface)?
- Can the intended audience identify the security action to be taken by the subject (e.g., shall process, shall display)?
- Can the intended audience identify the thing acted upon to reduce the likelihood of a threat to exploit a system vulnerability from this requirement?
- Can the intended audience identify the conditions under which the security action must take place (e.g., auto-logout after 10 minutes of idle activity)?
- Can this security requirement be verified by analysis, demonstration, inspection, or testing?
- What is the source of this security requirement (e.g., stakeholder, security risk assessment, regulation)?
- Does the security requirement identify the solution?
- Is the security requirement written as a positive statement such that it can be verified by analysis, demonstration, inspection, or test?

If the answer to any question is "no," the security controls identified in the risk assessment should be revisited to determine the intent and expected behavior. This cycle is continued until a concise statement is written to capture why the security control is required and what the system will do.

Below are three primary challenges to writing good security requirements:

a) Avoiding negative requirements: One of the most common challenges encountered is preventing negative requirements (e.g., "The system shall not allow unauthorized users."). Unfortunately, negative requirements make verification unattainable, because they require proving that the system will *never* allow a particular event, under any conditions. Thus, it is important to (a) correct the requirement language and (b) limit the scope of the system's requirement documents to what the system *does* do, not what the system does *not* do. If the intent of a negative requirement is to describe "what the system must do," try to substitute active verbs for the word "not." For example, the above could be rephrased as: "The system shall reject unauthorized users."

b) Human factors vs. security balance: The requirements must also provide an appropriate balance between the sometimes competing needs of security and human factors. It is common for a requirement that increases usability to also reduce overall system security and for the converse to occur. The security risk assessment for the medical system should drive the relative importance of each potential security requirement and guide the final balance reached.

c) Properly planned verification/validation: All requirements need to be written to allow them to be tested to ensure proper system operation. The following methods of confirmation should be considered during requirement generation:

    1) Verification by:

        i) **Analysis**: involves a technical evaluation of design information, such as equations, charts, graphs, drawings, schematics, and other data.

        ii) **Demonstration**: involves operation, manipulation, or adjustment of an item during performance of a function.

        iii) **Inspection**: involves physical examination of the item using the naked eye, tools, gauges, or other measuring devices.

        iv) **Test**: involves observation or recording of data during operation of an instrumented calibrated item.

    2) Validation of requirements through one of the following forms:

        i) **Actual Use Testing**: finished devices or components are placed in the actual operating environment (laboratory, hospital, clinic) and operated by trained users on actual patients, samples, etc.

        ii) **Simulated Use Testing**: finished devices or components are placed in a simulated use setting and operated by trained users on pre-screened individuals or derived samples representing a cross-section of the anticipated population.

In summary, cybersecurity requirements are clear, testable, and reference further detailed background to justify their need, such as a policy or compliance standard. Furthermore, per NIST Special Publication 800-53, security requirements include those requirements levied on a system that are derived from laws, executive orders, directives, policies, instructions, regulations, standards, guidelines, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. The following are examples of properly written security requirements for a use case that requires a medical device to send data via Bluetooth (as required by market specification) to a mobile device.

REQ 1: The system shall select radio antennas and calibrate transmission power levels to a maximum of 15 dBm.

Intent: Reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Reference: NIST SP800-53r4 AC-18(4), NIST SP800-121r1

REQ 2: The system shall utilize <XYZ> level encryption during data transmission.

Intent: Provide confidentiality to patient data during transit over the Bluetooth link.

Reference: NIST SP800-121r1

Annex D
(informative)

Questions that can be used to identify medical device security characteristics

Clause 4.2 of ANSI/AAMI/ISO 14971 requires that the manufacturer identify those characteristics of the medical device that could affect safety. Clause 4.2 of this TIR asks the manufacturer to indicate the intended use and identification of characteristics related to the security of the medical device. Taking these two directives as input, this annex strives to pose a series of questions designed to aid the manufacturer in defining the characteristics of the device that affect or are affected by security, the risks arising from these characteristics, and the design controls that may be put in place to mitigate those risks.

ANSI/AAMI/IEC 80001-2-2 introduces the concept of security capabilities for IT-networks incorporating medical devices, and it is this approach that provides the foundation for this annex which uses these capability classes to identify security vulnerabilities as outlined in 4.3 of this TIR.

If these questions are considered from the point of view of all the stakeholders involved (e.g., users, maintainers, patients, etc.), a more complete picture can emerge of where the security risks can be found. Once these have been identified, their impact on the safety of the device (hazards) must be assessed.

The list is not exhaustive, or representative of all medical devices, and the manufacturer is advised to add questions that can have applicability to the particular medical device and to skip questions that are not relevant to the particular medical device. The manufacturer is also advised to consider each question not only on its own but also in relation to others.

D.1 Essential performance

Essential performance, as defined in ANSI/AAMI ES60601-1 is described as the “performance of a clinical function, other than related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk”.

Evaluating essential performance is one technique that may be used to identify security risks with a safety impact. Extra security measures may be appropriate based on the specific capabilities, properties, asset, or attributes of the device, and the security controls designed into the device should keep these capabilities or assets (essential performance) secure.

a) What is the essential performance of the device?

    1) Is it a life-sustaining medical device?

        i) How is the device used to sustain life? Can the life-sustaining functions (essential performance) performed by the device be guaranteed in the event of a security breach or denial of service attack?

    2) Can unauthorized access, unauthorized activities, or loss of data affect essential performance?

b) Can the device be used to affect the patient? For example, warming, electrical impulses, x-rays, deliver fluids?

c) Is the medical device intended to modify the patient environment? Factors that should be considered include temperature, humidity, atmospheric gas composition, pressure, light.

    1) Is access to these functions controlled with the appropriate authorization controls?

d) Is the device implanted in a patient?

    1) How are instructions or measurements taken from the device while it is implanted in the patient? For example, from a physical access port implanted in the patient, or via a wireless connection?

    2) Can configuration or calibration of the device be modified while it is implanted?

e) Is the device intended to make medical decisions or support medical decisions made by a doctor?

1) What controls are in place to ensure the integrity of algorithms or data generated from algorithms used to make or suggest medical decisions?

2) Can the operation of the algorithm be affected by outside influences or the results be intercepted and changed? For example, if an automatic insulin pump detects that the patient needs another dose, what checks are in place to ensure that the device does not deliver an unnecessary or incorrect dose?

3) What controls are in place to ensure the integrity of measured or collected clinical or physiological data used to make or suggest medical decisions (e.g., diagnostic ECG data or ultrasound images)?

f) Does the device control other devices or is it controlled by other devices, either directly or remotely?

1) Can the device be used to impact the essential performance of other devices?

2) Does the device control other devices connected directly to the patient?

3) What is the impact if a security breach occurs on the controlling device, and allows an attacker to gain control of subsequent devices?

g) If present on a network, could the device be used as a launching pad (pivot point) for malware on the network?

h) Is there a process to check for known vulnerabilities and for applying fixes?

D.2 Data storage

A device's most valuable asset is often the data that is stored on it. Theft of PII is a common motivation, but the operation or integrity of the device itself can be compromised by tampering with the configuration data or measurements taken.

D.2.1 PII/Private data assets

a) Does the device store PII Data?

b) Is the data encrypted when at rest?

c) Are backups created and stored elsewhere?

1) Are backups encrypted?

2) Are they encrypted before transport or transmission to the other site?

3) Is there a limit on how long backups are kept or on how many versions are kept?

d) Is patient data scrubbed or obscured to remove personal information when not required?

e) How is the integrity of the data preserved on the device and during transfer?

f) Is the data encrypted when not at rest (i.e., in volatile memory)?

g) Is encryption fixed or configurable?

1) Is encryption based on a publicly recognized standard (recommended) or on a home-grown solution? For example., AES-256 vs. MyHashKeyEncryption

2) Is encryption/decryption tested against a validated compatible system?

3) How are keys managed?

h) Does the device use or maintain billing or financial information?

i) Do portions of the data have different levels of sensitivity (PII/non-PII)?

1) Is all data encrypted, or just PII?

2) Is any of the PII subject to additional restrictions according to local laws?

j) Can the data be classified according to sensitivity, and can the principle of least privilege be applied?

k) Is export of private data or PII (e.g. through removable media or the network) logged and attributable to an authenticated user in a security audit trail?

D.2.2 Non-PII data assets

a) What kinds of non-PII or personal data does the device store (e.g., diagnostic data or therapy parameters)?

b) Does the device store network or other user credentials that could be used to gain access to other systems? I.e., logon to a wireless network or authenticate to an LDAP or similar user authentication system?

c) Does the device store configuration or calibration data?

1) Is configuration or calibration data critical to the operation of the device or safety of the patient? For example, if calibration settings are changed, could it cause harm to the patient?

2) What is the impact if configuration data or controls (e.g., configuration interface menus) are compromised?

3) Are controls in place to ensure the integrity of the configuration data?

d) Are measurements taken? For example, the variables that are measured and the accuracy and the precision of the measurement results.

1) Can the measurement apparatus or data be compromised? What is the impact if they are?

2) Are controls in place to ensure the integrity of the measurements taken?

e) Does the device employ removable media?

1) Are storage devices on the device removable in any way? Removable may include both external and easily accessible storage media, and internal storage media such as hard drives. Consider methods by which someone may be able to attach removable media to copy data to or from the device, or if internal storage devices are easily accessible, removable, etc.

2) Is export of sensitive data logged in a security audit trail?

3) Is the user presented with a banner warning that cautions that data exported to removable media should be protected?

f) Are there any other methods to copy, remove, or place data on the device? Consider other methods that data could be copied to or from the device. Examples might include USB ports, PCIe ports (for removable PCIe drives), service ports, wireless access points, etc.

D.3 Data transfer

Data transfer refers to information (data) that is sent to or from the device. It is not concerned with the storage of the data on the device (volatile or nonvolatile), but with the actual data when “in motion” between endpoints.

a) What types of data are transferred to and from the device?

1) Does the data contain PII?

2) What methods could potentially be used to intercept data between endpoints?

3) Are controls in place to ensure the appropriate confidentiality, integrity, and authenticity of the data before and after transfer? For example, encryption and digital signatures.

b) If an adverse event occurs (either to the patient or the device), can the data be recovered or restored?

c) Is availability of the data transferred to or from the device critical to its operation?

1) If data transfer to/from the device is interrupted, does that interruption represent a safety risk?

2) If data transfer to/from the device is interrupted, is critical data cached so that it can be re-transmitted once connectivity is restored?

d) Does the device transfer data via wired connection?

1) What kinds of communication ports are available on the device?

i) Are communication ports based on standards? For example, standard Ethernet?

ii) Are there any proprietary communication ports?

iii) Are there serial (e.g., RS-232) ports available?

iv) Are communication ports internal or external to the device? Are they easily accessible?

v) Are communication ports enabled by default, or do they need to be enabled before they can be used?

e) Does the device transfer data via wireless?

1) What kinds of wireless connectivity does the device use? For example, Bluetooth, Wi-Fi, NFC, custom radio, etc.?

2) How are the wireless communications secured? Consider what standards are implemented and supported.

3) Can security levels be negotiated with the peer?

f) How are communication protocols (e.g., TCP/IP) implemented?

1) Are they implemented using COTS software or part of an underlying OTS operating system? Consider the selection of technologies based on the maturity of the implementation(s).

2) Are they implemented using a custom solution? Consider introducing more stringent testing processes to ensure the protocol stack is robust enough for deployment into a hostile operating environment, such as a hospital network.

i) How is the implementation verified in terms of standards for the protocol?

ii) Can it be verified or certified by an outside body?

D.4 Authentication & authorization

One of the most effective means of protecting a device and its operation is by authenticating the actors, human and machine, that interface with it and by ensuring that these actors are authorized for the function performed.

a) How does the device authenticate users or services?

1) Does the device/system have its own authentication storage/mechanism?

2) Does the device support/use a separate authentication provider? For example. Active Directory?

b) How are credentials managed?

1) Are credentials updated on a regular basis?

2) Are credentials updated via remote configuration change, or made locally?

c) Are there any hard-coded or default accounts on the device?

1) What is the purpose of the default or hard-coded accounts?

2) Can hard coded accounts be disabled or have their credentials changed by the end-user of the device?

d) How is credential expiration managed?

1) How often are users required to update their credentials?

2) Is credential expiration based on time, number of uses, or other?

3) Can the expiration of credentials be managed from the device? If so, what authority is required to configure it?

e) How does the device implement person authentication? That is does the device allow a person to authenticate with the device, via a login screen, remote session, or other method?

f) Does the device support multi-factor authentication?

g) How is authentication managed, based on the operating environment?

   1) Does the operating environment in which the device is to be used affect which authentication methods should be employed based on location, purpose of use, etc.? Examples might include different authentication methods in an emergency situation.

h) Does the device support multiple authorization levels or roles?

   1) Does the device implement the principle of least privilege?

   2) What systems are in place to prevent privilege escalation?

   3) How are privileges compartmentalized?

i) Do authenticated user sessions have a timeout? Consider the operating environment in which the device will be used. In some cases, different session timeouts may be necessary, or the ability to disable a timeout may be desirable.

j) Do user accounts become disabled after a certain number of failed login attempts?

   1) Are they re-enabled after a period of time to prevent attackers having a simple means to conduct a denial-of-service attack on accounts?

k) How are user accounts audited?

   1) Are there controls that disable accounts after a certain amount of inactivity (e.g., 3 months between logons) has passed?

l) How can audit reports of accounts be generated? Consider methods aside from centrally located authentication providers (e.g., LDAP) of generating lists of users from the device so that unnecessary user accounts may be deactivated.

m) Does the device authenticate with other systems/software/services, or allow other systems/software/services to authenticate with it?

   1) How does the device authenticate with other systems, and how do other systems authenticate with the device?

   2) How are credentials managed for system/software service authentication? For example, a remote system may require credentials that are not stored in an existing LDAP directory and must be coded into the software that authenticates with other systems. A good example of this is authentication with an external Web service.

   3) If credentials for authenticating with other systems are stored on the device, are they encrypted? If so, are best practices used to manage the decryption key?

   4) Are credentials stored in hardware (e.g., a TPM)?

D.5 Auditing

Essential to detecting an intrusion and to preventing intrusions is the process of logging and auditing the relevant events and activities. The audit data itself is an important asset.

a) What actions or activities are logged or audited on the device? Activities that should be considered include the following:

   1) all user, device, or process authentication activity;

   2) user actions/activity;

   3) changes to system configuration or calibration;

   4) system-level actions/activity (e.g., health of the device, sensor readings);

   5) network activity (e.g., remote network connections, data transferred to the device);

   6) software/firmware updates; and

   7) export of sensitive data.

b) How is audit data stored?

   1) Is the audit trail stored in clear-text, or encrypted?

   2) Where is the audit trail kept on the device and who has access to it?

   3) Can audit data be erased or otherwise tampered with?

   4) What are the limitations of audit data storage?

      i) Does the data have finite space in which it can be stored, and when that space is used up, the audit trail begins overwriting the oldest data?

   5) What authority is required to remove an audit record?

   6) Is audit data stored with system data?

c) Can audit data be transferred from the device?

   1) How is the audit data transferred? For example, via Infrared transfer, Network (wireless or wired), removable media.

   2) Is audit data encrypted prior to transfer?

   3) Are there methods to archive or back up audit data?

d) What mechanisms are in place to ensure that audit data is not tampered with during transfer?

e) Who is authorized to access audit data?

   1) Can audit data be read by anyone, or are the role-level controls to limit access?

f) Are there any other types of access to audit data?

D.6 Physical security

The simplest way of accessing a device is often proximity access, not remote. Malware can be accidentally introduced using personal devices (e.g., smart phones, USB drives). Data can be stolen by performing a screen dump, making a photograph, or taking a disk drive.

a) What physical properties does the device exhibit that allow access to information, data, etc., on the device? For example, accessible Ethernet or USB ports, removable hard drives, etc.

b) Does the device have externally accessible data ports? For example, network ports, serial ports, USB ports.

   1) Are external ports enabled by default?

   2) Can external ports be disabled?

   3) When external ports are used, is the activity audited or logged?

   4) Are there physical locks or other mechanisms available to block access to external ports?

c) Does the device have a screen?

   1) Is data displayed on the screen sensitive in nature? For example, are passwords displayed in clear-text?

   2) Is patient data viewable on the screen? Clear text or encrypted/hidden?

   3) Is the device intended to be used in a public area?

d) Are there any internal ports on the device? For example, internal USB connections, JTAG connectors, debugging ports?

   1) Are internal ports disabled, either via hardware (e.g., jumpers) or software controls?

   2) Can debugging ports be disabled in production configuration of the device?

e) Are there any anti-tampering mechanisms on the device?

1) Is there any way to detect physical intrusion into a device, actively or passively? For example, labels, adhesives, tamper evident seals, physical covers.

2) Are there software or electronic mechanisms to detect intrusion into a device?

D.7 Device/system updates

Device manufacturers should place great emphasis on their strategy for providing updates and to ensure that only authentic updates are made.

a) Can updates be performed remotely?

   1) How does the device owner obtain software updates for the device? For example, downloaded over the Internet, provided on CD or USB drive.

      i) If software updates are downloaded over the Internet, how is the authenticity of the download confirmed? For example, secure hash, keyed hashed message authentication code, or digital signature?

      ii) If software updates are provided on removable media, how is the authenticity of the software confirmed?

      iii) When software updates are provided, what controls are in place to ensure the media (downloaded or otherwise) is free of malware/viruses?

b) Are software updates performed physically (in-person) by the manufacturer? For example, using a specific fixture or hardware required to apply the software update.

   1) Are any other physical controls in place to ensure that software updates to the device can be performed only by the manufacturer or trained service provider? For example, USB dongle required to authenticate with the device before software updates can be applied.

   2) Are application updates and operating system updates handled separately or bundled?

c) Is the authenticity of a software update checked before it is applied? For example, does the device require signing of software updates?

d) Are software updates validated in any other way prior to installation on the device? For example, deep inspection of the software update for specific design features.

e) Once software updates are installed on the device, what measures are in place to roll-back an update if an unsafe condition occurs?

f) Can the configuration of the device be altered either remotely (e.g., over a network) or physically on the device?

   1) What method (e.g., physical access or network) is used to alter the device configuration?

   2) What kinds of changes can be made to the configuration of the device?

   3) Can configuration changes place the device in an unsafe state?

   4) Could configuration changes affect patient safety?

   5) Can the configuration of the device be returned to a known safe state after being changed?

   6) What authentication controls are in place to limit access to configuration changes?

   7) Are configuration changes validated prior to being applied?

   8) Are device configuration changes validated prior to being applied? For example, are the changes within known safe limits on the device?

   9) Can configuration settings affect user access or privileges?

g) Does the device use COTS operating system or software?

   1) What is the verification/validation strategy for COTS software updates?

   2) Are COTS software updates applied by the manufacturer or the device owner?

3) How often are COTS software updates made to the device?

4) Are there special dispensations for applying critical security updates to the COTS software? For example, hotfixes or zero-day security fixes.

h) Are any other COTS or Software of Unknown Provenance (SOUP) used as part of the device?

1) Have COTS or SOUP components been evaluated from a security standpoint?

i) Is there a process for monitoring security issues related to your device after-market?

j) Is there a process whereby users can report a security issue with the device?

k) Are COTS and other components used in the device monitored for security updates?

l) Is there a response process for when security issues are detected? Any process should analyze the security issue and recommend a course of action commensurate with the safety and security risks.

D.8 Hardening

The easiest method of preventing a function from being compromised is to remove that function. Identify applications, access points, and services that are not required for normal operation and remove or disable them.

a) What measures are taken to ensure the system is hardened from external access via exposed interfaces? For example, network connections (wired or wireless), proximal access (physical access to the device).

b) Have unused or unnecessary user accounts been disabled on the device? For example, operating system “guest” accounts, database administrative accounts with default passwords.

1) What accounts are necessary for the intended operation of the device or system?

2) Have credentials for default accounts been changed?

c) Are any custom software applications or services installed on the device?

1) What account/access level do those services execute under?

2) Do those accounts have their privilege levels configured as to not allow them to execute in unintended ways?

d) Does the system use a COTS operating system or software? For example, Windows, Oracle.

1) Have resources such as the National Checklist Program Repository, NIST SP 800-70 (see Bibliography [58]), been reviewed for guidance regarding configuration of operating systems and off-the-shelf software?

2) What measures are taken to ensure that COTS software has been hardened on the device as to not allow inappropriate access, escalation of privilege, etc.?

e) How is device integrity ensured post manufacturing?

1) Are there controls in place to ensure that the device is not tampered with during transport or delivery?

2) How do you ensure integrity of software updates or other installation media after it is delivered? For example, hashes, digital signatures?

f) How is the integrity of the device ensured when it is initially connected to a network for the first time? For example, are there methods to ensure that zero-day or recently identified vulnerabilities that have active agents looking to exploit those vulnerabilities (worms, viruses, etc.) cannot infect the device when it is first connected to the network?

g) Are there adequate controls to ensure that malware, viruses, or other unwanted software is not introduced on the device or a component of the device during manufacture or assembly?

1) Is there an audit policy in place as part of the manufacturing process to continually monitor these controls?

h) Have components been evaluated against databases of known vulnerabilities (e.g., CVE)?

D.9 Emergency access

Where a device supports emergency access, consider the security ramifications.

a) Is there a need for emergency access given the intended use of the device?

b) Does the device implement emergency access features (e.g., “break glass” functionality)?

c) What actions are allowed when operating in emergency-access mode? For example, can the user operate the device in a limited capacity, change settings, update software?

d) What is the intended purpose of the emergency mode? For example, is it to use the device for a limited time or a limited set of features in an emergency situation?

e) What kinds of changes might be made to the device while in emergency mode?

f) What kinds of information or assets can the operator access while in emergency access mode? For example, PII data, user credentials, other sensitive information.

g) Can an operator update the operating system or software on the device in emergency access mode?

h) What actions are logged or audited when operating in emergency-access mode?

   1) Are audit data or logs accessible during emergency use?

   2) Can audit data or logs be modified during emergency use?

   3) Are additional actions audited or logged that are not during normal operation?

   4) What detail level are actions audited at, when operating in emergency access mode? Is it possible to audit in a higher level of detail when operating in emergency-access mode?

i) What constraints are placed on emergency access that enforce expected behavior?

D.10 Malware/virus protection

Devices often include or support the installation of malware or intrusion detection and prevention applications.

a) Is the device susceptible to viruses or malware? For example, does it operate using a COTS operating system or similar that is known to have malware or viruses?

b) Does the device employ malware or virus protection software?

   1) How often are virus or malware definitions updated or deployed to the device?

c) Are there other controls on the device to prevent malware, virus, or other unwanted modifications?

d) Does the device include Intrusion Detection or Prevention systems (IDS/IPS)?

   1) How often are IDS/IPS signatures updated on the device?

   2) How are those IDS/IPS signature updates deployed?

e) Does the device use application or process whitelisting?

   1) How are changes to the whitelist performed?

f) What level of access is required to install, modify, remove, or disable malware or other protection measures?

   1) Are modifications to malware, virus, or other security protections logged?

   2) Does the design define how malware or intrusion protection logs are reviewed or transmitted?

g) Does the design consider potential coexistence of protection applications (e.g., malware monitoring or intrusion detection) with the system software and applications?

D.11 Backup/disaster recovery

Performing a restoration or disaster recovery should not result in a security compromise of the device, nor should the backed-up data itself be easily compromised.

a) What methods/processes are used to ensure security of device or system backups?

b) How is the confidentiality of data on device backups ensured?

   1) Are device backups encrypted?

   2) Are there other security measures to ensure confidentiality of backup data?

c) How is the integrity of device backups ensured?

   1) Are there multiple backups that can be compared?

   2) Are there hash values or similar mechanisms produced for each backup to ensure integrity?

d) After a device is restored using a device backup, what processes or procedures are in place to validate that the device has been returned to a known good state.

D.12 Labeling

Without proper instructions for use with respect to security, the user may not be able to use the security features or may in fact unwittingly work against them.

a) What instructions are provided for the secure use of the device?

   1) If there is sensitive information (e.g., PII) displayed on the screen, are there instructions on the proper use of the device to ensure such data is not publicly visible? For example, ensuring the device is turned away from publicly accessible spaces if it contains PII.

   2) Are there instructions or labeling available that provide instruction on the use of the device in different operating environments? For example, documentation describing the differences in how a device may operate when in an acute care setting vs. other settings.

b) Are instructions provided for the secure configuration and deployment of the device?

   1) What configuration(s) of the device are considered “secure” in different operating environments?

   2) Is there a baseline or recommended network configuration to support secure deployment of the device?

   3) Are there configuration settings that network administrators need to be aware of for the device to function properly? For example, network firewalls may need to be configured to allow certain open ports.

c) What instructions are provided for the secure disposal of the device?

   1) Is there sensitive information stored on the device, such as PII or other confidential information?

   2) Are instructions provided for how to properly dispose of the device once it has reached the end of its functional life to ensure that data stored on the device is also destroyed appropriately?

Annex E
(informative)

Security risk examples applied to a medical device

This annex provides a proxy for the security-related activities that occur during product development. The intent is to provide development engineers with examples and learning opportunities that re-enforce the prior materials in this document.

This Annex consists of the following components:

- A fictional system, the Kidneato artificial implantable kidney, provides a platform for the discussion of security issues and techniques. Keep in mind that this specific example can also represent a wide range of medical devices and accessories. For example, the “Kidneato Programmer” fits into a controlled network where one might find a CT scanner, infusion pump, or other medical device.
- A cyber hygiene example that provides a partial list of good security practices designers and users of a system should follow.
- A security analysis using risk methodology.
- Risk analysis of an implanted medical device communication design decision.
- An example implementation of a medical device communication accessory.

The example implementation follows a format where:

- An initial design is implemented using good engineering practices without regard to the recommendations of this document;
- an example of how the implementation is viewed from the attacker’s perspective;
- potential impact from the attack;
- an analysis of factors that enabled the attack and how recommendations of this document would have prevented the possibility of this attack;
- security risk controls that could be applied to the initial design to reduce the cybersecurity risks.

The example implementation asks readers open-ended questions. This helps the reader better understand the attacker’s thinking and methods while encouraging them to apply the questions to their own work. Unfortunately, there is no single correct solution for any situation or implementation. These questions should help extend the example to cover a broader perspective.

E.1 The Kidneato System

The purpose of this example product is to illustrate a specific example, the Kidneato, but to also represent a wide array of products. The location, communication, processing, data storage are of primary importance, rather than the specific medical function. Besides representing the Kidneato programmer for the following examples, the Network-connected Medical Instrument could also be viewed as network-connected capital equipment (i.e., CT scanner, radiation treatment, infusion pumps, anesthesia, heart bypass pump, digital X-ray, and other medical devices).

Non-capital equipment may be part of a manufactured accessory kit or it may be patient-supplied such as a personal smart phone, or wireless scale. The Kidneato system consists of an implanted medical device along with accessories that support the implant and subsequent operation of the medical device. Block diagrams of the Kidneato system are provided in Figures E.1 and E.2.

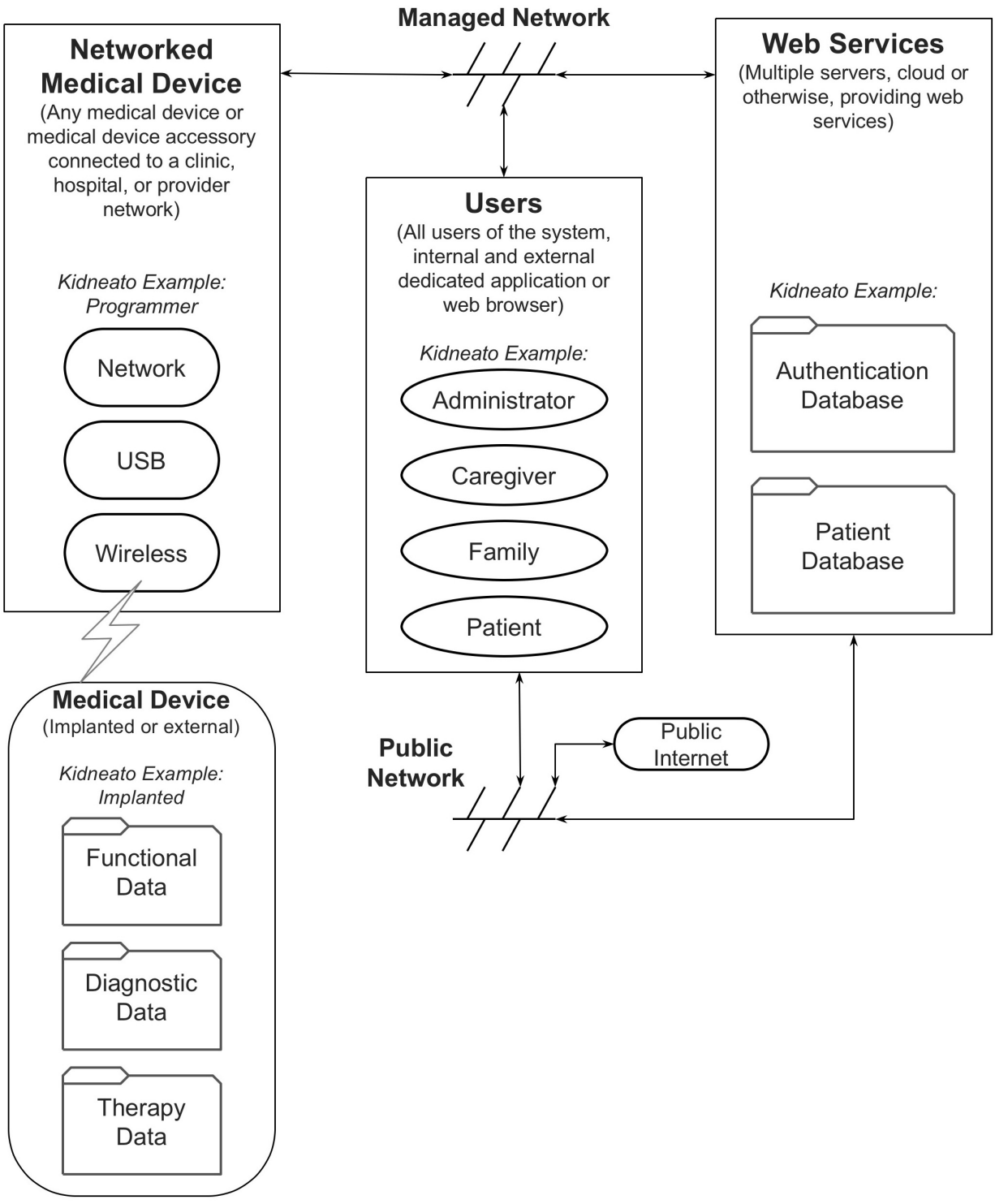

Figure E.1- Block diagram of the Kidneato system, managed environment

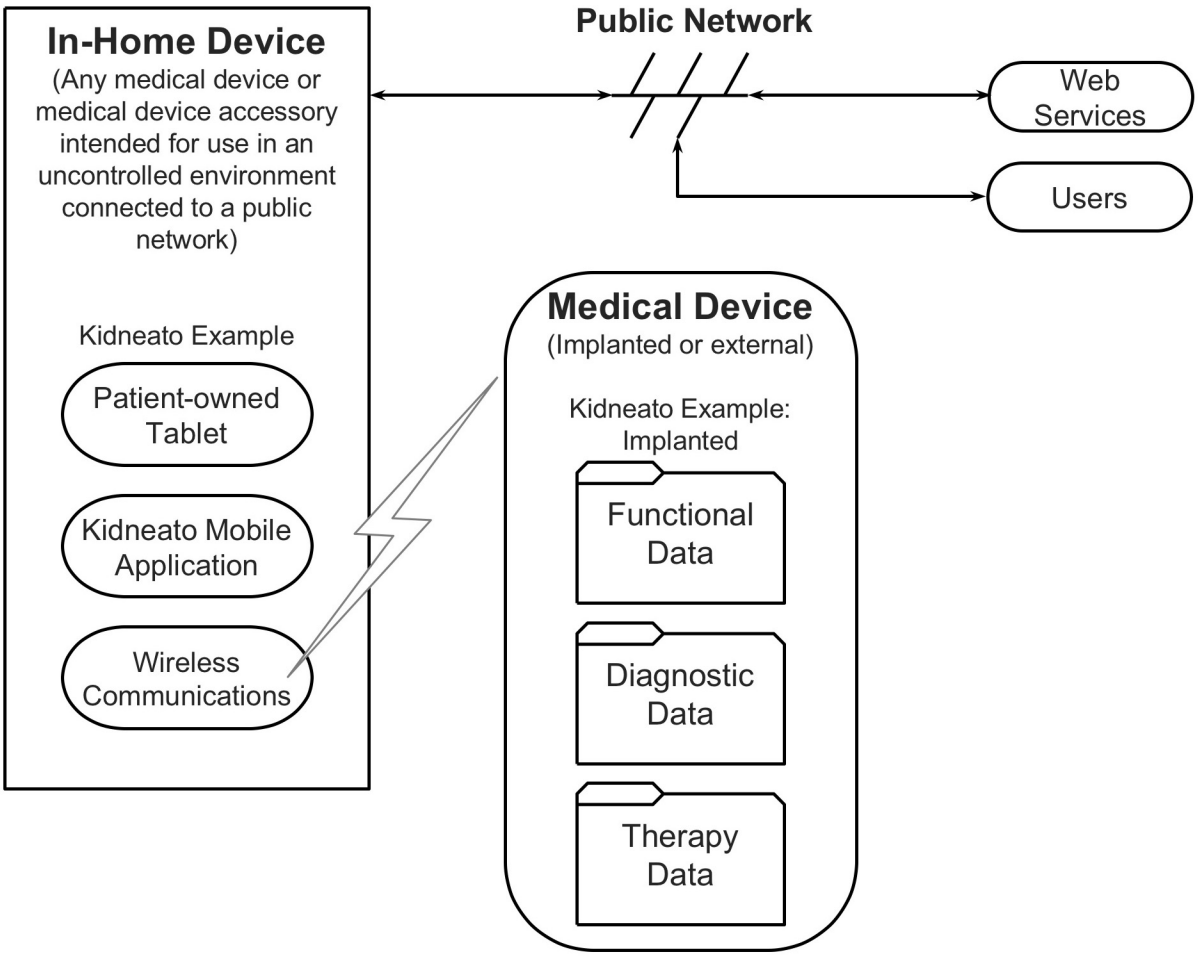

Figure E.2 – Block diagram of the Kidneato system, patient environment

The Kidneato is a therapy and diagnostic implant. It is configured and tested at implant and again prior to patient discharge. It is subsequently managed by the patient, caregiver, HDO, or family member through a combination of remote (non-clinical setting) and clinic follow-ups.

Each Kidneato has an identifier established during manufacturing and cannot be changed. This identifier is associated with a patient master account and HDO master account to administer and monitor the medical device through web services.

Web services are not required to manage the device. Without web services, the device history is limited to printed reports generated when an HDO interacts with the patient.

The Kidneato has a wireless interface that allows it to communicate with system components provided by the manufacturer. The following information is sent and received:

a) Transmit diagnostic information

   1) Patient information

   2) Disease

   3) Device status

b) Receive commands and information

   1) Request information

   2) Set patient information

   3) Set alert parameters

   4) Set therapy parameters

   5) Set calibration parameters (factory only)

   6) Update bootloader (factory only)

   7) Update firmware (factory or field)

c) During its operation, the Kidneato:

   1) Provides therapy;

   2) Monitors and records device and patient information;

   3) Generates alerts;

   4) Transmits and receives data; and

   5) Battery is recharged through an inductive charger.

E.2 Kidneato programmer

The programmer is provided by the device manufacturer as a leased or purchased accessory. Its only function is as a Kidneato accessory. It is used by trained personnel during device implant and subsequent in-clinic follow-up/device check. Service or updates (including software) are provided by the manufacturer.

In the Kidneato examples, this subsystem is used to interact with the Kidneato implant. From a security perspective, it also represents any medical device or accessory in the clinic or hospital that is connected to a network.

The programmer has the following features:

a) Remote (in-room) display of main screen

b) Ethernet, Wi-Fi, and optional cellular communications

   1) Communicates with Web Services (local or cloud)

   2) Communicates with local printers

   3) Controlled from a remote location

   4) Storage of reports/data (WebDAV, SFTP, etc.)

   5) Software and firmware updates

   6) Remote services for maintenance by the manufacturer via back-end infrastructure

c) USB (mass storage)

   1) Storage of reports/data

   2) Firmware update of the medical device

   3) Software update of the Programmer

d) USB (serial port emulation)

   1) Service/debug port for use by the manufacturer

e) USB (HID)

   1) Human input device, such as keyboard or mouse

E.3 In-home monitor (IHM)

The IHM is used by the patient or caregiver when the patient is away from the clinic or hospital. Primary users are the patient or nurse with only minimal training.

In the Kidneato examples, this subsystem is used to interact with the Kidneato implant. From a security perspective, it also represents any medical device or accessory that may or may not be patient owned and is located outside of the clinic or hospital environment and is connected to a public network.

The IHM utilizes a user-purchased OTS computing device, such as a tablet or a PC (referred to as “Tablet”). An application software accessory is downloaded from an appropriate source and installed on the computing device by the user or owner. The software accessory is capable of communications with the implanted device via wireless signaling to an inductive communication Wireless Communication Accessory (WCA) that is also used for recharging the implanted medical device. Communications between the Tablet and WCA are conducted using conventional means, such as a Bluetooth connection.

a) Medical Device Communications
    1) Mutual induction to implanted device
    2) Bi-directional communications
    3) High-power downlink mode to recharge battery
b) Tablet/ WCA Communications
    1) Wireless Bluetooth communications between Tablet and WCA
    2) Bluetooth pairing with tablet and WCA
    3) Ability to update WCA firmware from Tablet
c) WCA Operation
    1) Battery operated
    2) Rechargeable via conventional USB charging port
    3) LEDs and beeper indicate status
    4) Button to turn on/off
    5) No alphanumeric display

E.4 Web services

Web services provide a central repository for data related to the medical device. This is a specialized medical device requiring web services beyond the scope of an Electronic Health Record (EHR) system.

In the Kidneato examples, this subsystem is shown to have specific capabilities. From a security perspective, it also represents any type of service that has public incoming and outgoing connections in a hosting solution, including “cloud hosting.” The subsystem may or may not include PII and Class III software.

Web services are implemented using a cloud-based architecture that is scalable and redundant. The services are built upon existing technology for the foundation and only minimal code is created to hook the foundational technologies together and to provide specific services related to the medical device and its users.

a) Communication
    1) Programmer
        i) Downloads medical device firmware updates
        ii) Downloads programmer firmware updates
        iii) Downloads firmware for new products
        iv) Uploads implant information

v) Uploads follow-up information

vi) Downloads historical data, analysis, recommendations

vii) Communicates with Web Services via Internet connections

2) In-Home Monitor

3) EHR Access

i) Web Services provides an API for integration with EHRs

4) Administrator Access

5) HDO Access

6) Patient Access

7) Caregiver Access

8) Family Access - iPhone, etc.

b) Data

1) Patient identification

2) Patient history

3) Device information

4) Device history

5) Therapy history

6) Transaction history

7) Reports

8) Event history

9) Anonymized research data

E.5 Web services - Direct access

Web services are made available to individuals through a software accessory that is installed on a computing platform of the user's choosing (PC, tablet, etc.). The accessory software communicates with Web Services via a screen and input device. Requests or instructions from the individual are communicated via the Web Services interface. Received data is rendered on the screen and or provided for printing or local storage (pdf).

Accessory software is downloaded by the user through the appropriate Internet service (Apple App Store, Apple Mac Store, Google Store, or PC download site).

The user authenticates via a user name and password. The user name and password are also used to determine the user's level of authority:

a) Administrator

1) Administers the hospital, clinic, caregiver, and additional administrator accounts.

2) Can view/enter administrative data.

b) Medical Provider (Health Delivery Organization)

1) Uses provided account to access medical data, change therapy, and read/write notes.

c) Caregiver

1) Uses provided account to access medical data and write notes, read responses.

d) Patient

1) Uses manufacturer-provided account to view a high-level summary and communications with their provider.

2) Provides family access.

e) Family

1) View high-level summary data.

E.6 Web services - Instrument access

The programmer and home monitor communicate directly with a web services API intended for machine access.

Each instrument carries a unique identifier determined during manufacturing.

API features include:

- Authenticated connection;
- Send queued messages to the instrument;
- Receive messages and data from the instrument that are queued for subsequent processing;
- Mediates remote control of the Programmer between a PC and the Programmer; and
- Asset management.

E.7 Example implementations

We will now implement various security aspects of the Kidneato implantable medical device and its accessories. Each example will use good engineering practices. We will then examine how good engineering practices without application of the principles described in this document can lead to an insecure system. The implementation will then be modified using good security practices to show how the security of the system has been improved.

E.7.1 Example #1 Basic Cyber Hygiene

The security risks in this example are associated with supporting the basic cyber hygiene needs of customers to prevent, detect, and respond to cybersecurity incidents. Some basic cyber hygiene items are listed, and then the Kidneato system is used to highlight how without basic cyber hygiene, a system is insecure.

The following list represents common cyber hygiene items that have been called out throughout this document. Many of the references listed at the end of this document refer to these items [15][36][50]. The following are common cyber hygiene needs:

- changing default passwords;
- enforcing password complexity policies;
- using authenticated and encrypted communications;
- disabling unused services, including interfaces intended for debugging;
- assigning user privileges appropriate to the user's authority;
- authenticating software updates;
- inventorying authorized and unauthorized devices;
- inventorying authorized and unauthorized software;
- ensuring that software was developed using best practices for the language and execution environment;
- developing and managing secure configurations for all devices;
- conducting continuous (automated) vulnerability assessment and remediation;
- actively managing and controlling the use of administrative privileges;
- regularly updating all software, operating systems, and apps; and
- regularly revisiting the top security priorities.

E.7.1.1 Security analysis

Risk methodology

The security risks are associated with supporting the basic needs of customers to prevent, detect, and respond to cybersecurity incidents. The risk methodology uses a five-point rating system – Very Low, Low, Moderate, High, and Very High, for both Likelihood and Impact. The definitions for these ratings were drawn from Table I-2 in NIST SP800-30 Revision 1 (see Bibliography [53]) and have been captured in the Kidneato development process and documented in the Security Risk Management Plan.

The following represents common cyber hygiene needs based upon the information in this TIR. The risks are all unacceptable without additional actions taken. The risk control measures are necessary to reduce the cyber hygiene risks to an acceptable level.

E.7.1.2 Security risk evaluation

This subclause presents a simplified security risk evaluation based on Table I-5 in NIST SP 800-30 Revision 1 (see Bibliography [53]).

Table E.1 - Security risk evaluation table

Vulnerability	Likelihood of Occurrence	Impact	Security Risk	Risk Control Measure
Kidneato Web Services does not enforce complex passwords. Users can choose a 6-character password, such as “123456”.	Very High This is a common attack with accessible attack surfaces.	High Unauthorized users can gain access by performing password guessing attacks.	Very High	Enforce unique, complex passwords
The Administrator password is the same for all deployments of the Kidneato Web Services component. Default password becomes publicly available through documentation provided by manufacturer.	Very High This is a common attack with accessible attack surfaces.	High Unauthorized users can gain access by scanning the internet for exposed systems and using default credentials.	Very High	Ensure default credentials are changed
All In-Home Monitors use the same credentials to access Kidneato services.	Moderate Requires a multi-step approach to compromise.	Moderate One Home Monitor can access data destined for a different home monitor by changing the serial number sent to the Kidneato services. This could result in unauthorized disclosure of patient data.	Moderate	Assign access privileges appropriate to the user role; one monitor must not be able to access another monitors data.

Vulnerability	Likelihood of Occurrence	Impact	Security Risk	Risk Control Measure
In-Home Monitors store Kidneato credentials in plaintext	Moderate Requires reverse engineering a software image, as well as gaining access to a software image.	Moderate By analyzing a software update image acquired over the internet, an attacker gains access to the credentials needed to impersonate all In-Home Monitors.	Moderate	Store authentication credentials in encrypted format.
The Kidneato Programmer is not hardened because it will reside in a hospital-controlled network. Things like network scans are not anticipated, a remotely accessible service interface is left enabled, and all applications run with administrator privileges.	High Networks in hospitals are frequently compromised.	Moderate The hospital network operating environment is not controlled. The Programmer is exposed to network scans from both legitimate users performing normal network discovery operations, and illegitimate users searching for additional attack targets. The service interface is discovered and available for further attack. A successful attack can modify the machine because it has administrator privileges.	Moderate	System hardening, leveraging resources such as National Checklist Program Repository, to turn off service interfaces and run in least privilege mode.
The Kidneato Programmer does not keep logs of access through the service interface.	High Networks in hospitals are frequently compromised.	Low A Health Delivery Organization needs to understand the extent of a compromise to facilitate mandatory reporting requirements. Patient safety is not directly impacted by lack of logs.	Low	Add logging for all security related events, such as remote access, network configuration changes, and user additions.

Vulnerability	Likelihood of Occurrence	Impact	Security Risk	Risk Control Measure
The Kidneato Programmer service interface is not disabled, even though configuration changes are available to turn it off.	High Users are unaware of all the interfaces.	Moderate The HDO administrators are unaware that the service interface exists on the Programmer, and as a result do not disable the interface.	Moderate	Disable service interface in released version. OR Provide information for secure use, noting the availability of the service interface and how to disable it.
The Kidneato Web Services do not receive regular security patches, even though the system is built on a commercial off-the-shelf operating system that has vulnerabilities published on a monthly basis.	High Systems are easily compromised with published exploits that have made it into common attack toolsets.	High HDO administrators are unable to patch the system, because they cannot fully verify the new functionality. Kidneato does not provide secure patches at the same rate as the commercial operating system, leaving a window of opportunity for attackers to exploit.	Moderate	Provide regular updates for security vulnerabilities
Software updates deliver malware through USB media.	Moderate USB media is used to deliver software updates and may become compromised as part of use with other workstations.	Very High The malware causes the system to behave unpredictably.	High	Authenticate software updates using a digital signature.

Vulnerability	Likelihood of Occurrence	Impact	Security Risk	Risk Control Measure
Kidneato programmer service interface uses Telnet for debugging purposes	High Networks in hospitals are frequently compromised.	Moderate Accessing the programmer remotely for service transmits both user credentials and patient data in plaintext. An attacker with network access is able to capture and analyze the data, resulting in disclosure of sensitive data.	Moderate	Use SSH for remote access, and enforce unique, complex passwords for all access.

E.7.2 Example #2 Implant Communications

E.7.2.1 Security analysis

When the Implant connects with the WCA, the Implant and the WCA wireless systems are designed to provide integrity with CRCs. The WCA and Implant use a static unique identifier with each transmission to provide authentication. The wireless communications are not cryptographically encrypted or authenticated.

The wireless communications may be initiated from a distance of up to 30 meters.

E.7.2.2 Security risk

An attacker within range can establish wireless communications with the implant. The attacker may do so in order to extract patient data from the implant, or modify the therapy delivery logic in the implant. The attacker must be within range and be able to impersonate a legitimate device by knowing the unique identifier and the data packets, which are both available for recording through eavesdropping on a legitimate session. The attacker may then replay the data as is. The attacker may also modify the data by changing the unique identifier and the corresponding CRC.

E.7.2.3 Likelihood

The likelihood is classified as Medium for the following reasons:

- The attacker may initiate this from a distance
- The attacker may accomplish an attack by replaying captured or modified traffic. Either of these attacks is accessible to an attacker who is moderately familiar with wireless techniques.
- The attacker can acquire the necessary equipment at relatively low cost.

E.7.2.4 Impact

The impact has two different classifications, depending upon the goal of the attacker.

Patient data disclosure is classified as Medium because it leaks sensitive information, but the information does not cause any harm.

Patient therapy modification is classified as High because it could result in inappropriate therapy being delivered to the patient.

E.7.2.5 Risk estimation

Describe the results that the attacker was able to achieve.

Table E.2 - Risk estimation analysis example

Risk ID	Asset	Threat	Vulnerability or Flaw	Likelihood	Impact
1	Patient Data	Attacker reads patient data	Lack of encryption on transmitted data	Medium	Medium Disclosure of patient data.
2	Patient Therapy	Attacker manipulates patient therapy by replaying legitimate commands	Lack of authentication on transmitted data	Medium	High Inappropriate therapy may be delivered.

E.7.2.6 Implemented control

Risk 2, modification to patient therapy can be addressed by requiring authentication. A possible solution is to add authentication through application of cryptography. Introducing correct use of cryptographic authentication provides assurances that the data is coming from a legitimate WCA, and it also provides message freshness to provide assurances that the data is not simply replayed.

Risk 1, the disclosure of patient data can also be addressed through the application of cryptography to provide confidentiality.

E.7.2.7 Residual risk estimation

Introduction of the cryptographic authentication and encryption reduces the likelihood of each risk, because an attacker must acquire the key to appropriately encrypt or decrypt the data. The keys are available only to legitimate devices, and as a result the attacker cannot simply sniff wireless traffic and modify or replay it. The attacker either needs to brute force the key, which will likely take longer than the therapy communication, or they need to acquire the key through reverse engineering either the Implant or the WCA.

Table E.3 - Residual risk estimation analysis example

Risk ID	Threat	Action	Post Mitigation Likelihood	Post Mitigation Impact	Rationale
1	Attacker reads patient data	Cryptographic Encryption	Low	Medium	Reading the data requires the attacker to have the key, which is only available to legitimate devices.
2	Attacker manipulates patient therapy by replaying legitimate commands	Cryptographic Authentication	Low	High	Replaying or modifying the wireless data requires the attacker to have the key, which is only available to legitimate devices.

E.7.2.8 New risk identification

The application of the cryptography has now introduced a new risk, whereby a legitimate user of the system is unable to communicate with the device to deliver therapy because they do not have the key. This new risk may have safety

consequences, and must feed into the safety risk management process. The factors responsible for the legitimate user to not have the key need to be understood, such as data corruption or broken equipment.

E.7.3 Example #3 WCA Firmware Update

The purpose of this example is to demonstrate two possible outcomes from a feature design: when good engineering practices are used; and when good engineering practices are combined with the guidance from this document. In the first case, a safe and reliable feature is produced in the absence of a malicious user. The malicious user, however, is not interested in how well the product performs according to its intent; he is interested in discovering emergent or other unspecified behaviors that can be used to attack the product.

E.7.3.1 Initial Design

The Home Monitor WCA has firmware that must be periodically updated. The update is stored on a cloud server that communicates with the Tablet. The initial design works as follows.

a) The Tablet Application uses Bluetooth to determine if the WCA is available. If it is, it requests secure communication using a stored and previously established key. This key was created when the WCA was initially paired with Tablet by transmitting it over a wired USB connection. Once communication is established, the Tablet determines the identity of the WCA and its firmware version.

   The wired connection is a "side channel" used to communicate with the key. If the key is known to the attacker, then he can communicate with the WCA.

   Design Considerations: What characteristics should the key have? Should it be randomly generated? If so, how should that be done? What happens to the severity of the risk if all WCAs use the same, randomly generated key?

b) When the Tablet Application is started, it connects with the server and authenticates using the UserID and Password previously entered by the patient. (The app saves the password to minimize use friction with the patient.) Once the tablet is authenticated with the server, a secure connection is made using the current best practice (e.g., TLS).

   This is a common problem. Both the objective (signing on) and the key to that objective are stored on the same tablet, which means the attacker has everything they need if they have access to the tablet. Consequently, security is entirely dependent on the security of the tablet's hardware and software, and lack of physical access.

   Design Considerations: How should the password be saved? Does encrypting it help? What should the minimum protections be? (It may help to draw a simplified diagram showing the Tablet and all the possible access points.)

c) The Tablet transmits its identity (including software version) along with the WCA's ID to the server. If an update is required, the server sends the update to the Tablet. The Tablet then sends the update to the WCA over the secure channel. The WCA validates the update, reprograms flash memory, and restarts.

   Communications between the server and the tablet are encrypted and cannot be intercepted by an attacker unless they have the key.

   Design Considerations: Is transmission encryption sufficient protection? Does this authenticate the software update? How would you use the best practices in Annex A to improve the security of the update process? Does this process violate any of the basic security design principles? What components external to our system do we need to trust? Is there some way we could design this so we don't have to trust components outside of our control? (Try answering the questions in Annex D.)

E.7.3.2 Attack of the Design

For this subclause we switch our perspective to that of the attacker. The objective of the attacker is to access the implanted medical device, retrieve confidential information, and/or change the settings on the medical device. At greater risk, the attacker can get close enough to monitor Bluetooth communications (range is about 30 meters), but there is less risk to attack from a greater distance.

a) The attacker recognizes that the Tablet is performing one-way authentication with the server. The Tablet has no idea if the server is correct or if it is malicious. The attacker monitors the network that the Tablet is connected to (Wi-Fi or LAN) and intercepts DNS queries from the Tablet for the IP address of the server. The attacker responds with the IP address of their own server to which the Tablet sends its UserID and

Password. The attacker now has the Tablet's login credentials and is able to communicate with the Tablet as if it were the authorized server.

Design Considerations: Did you consider a Man-In-The-Middle (MITM) attack? If not, what was missing from your analysis that caused this to be missed? Hint: The security architecture needs to have a view that shows all of the possible system access points.

b) The malicious server receives the firmware and software versions. Because the WCA can be purchased on the used market, the attacker has been able to reverse engineer the hardware and rewrite the firmware. This "updated" firmware is then sent to the Tablet, which is subsequently sent to the WCA and the WCA updates itself. This accomplishes two things: 1) the attacker now has control of the WCA and; 2) the WCA may not be updatable by the manufacturer because the attacker has used a higher version number.

Design Considerations: What security practice would have prevented this?

c) Similarly, the attacker downloads the medical device accessory application used in the Tablet from the Tablet's app store. This allows the attacker to reverse engineer the app and make minor modifications. This "updated" app is then used by the Tablet. The attacker can now control the Tablet from any location on the Internet through a back-door she has installed.

Design Considerations: What can an attacker learn from a published application? Consider the various types of assets discussed in the TIR. How could a published application benefit a new start-up or competitor? What is it about a published application that makes it vulnerable? What can be done to the published application to reduce the security risk? How would you proceed with a risk assessment to determine if mitigations were required for the application?

d) Alternatively, the Tablet may not allow app updates except from the App Store. The attacker places their modified version of the app in the App Store and causes it to look like the manufacturer's official app. Some percentage of the patients will download the wrong app, thus giving the attacker control of random medical devices that may be a great distance from the attacker.

Design Considerations: What role does social engineering play in the system? Does your system view include the appropriate actors? How could social engineering attacks be effective against these actors? Should social engineering be considered in the security risk management analysis? How would you estimate the viability of a social engineering attack?

E.7.3.3 Results from the Attack

In this subclause, some of the possible consequences of vulnerability exploitation are considered.
In steps 1-3, the attacker has been able to achieve complete control of the accessories of a specific patient, but was required to be relatively close to the patient. Having complete control, the attacker can perform a remote attack at a later time or can program the WCA to perform the attack at a later time or upon a certain event trigger.

Step 4 allows the attacker to gain control of random medical device accessories. While they do not have control over which patients are affected, they may be able to hold the manufacturer hostage or create a decline in the manufacturer's valuation.

The attacker can use Step 4 to attack a specific patient by using social engineering. The attacker contacts the patient claiming to be a representative of the manufacturer or provider. They tell the patient that their app needs to be updated and to delete the current app and install their malicious app.

E.7.3.4 Analysis

This broad and effective attack was made possible because the designers focused on meeting traditional product requirements that are based on a definition of normal or expected use that did not include security risk. They did not consider that a different actor, a malicious user, could use the product features against the best interest of the patient. Part of the problem was that the product was developed by different design teams assigned to different components of the product. Assumptions were made, but not confirmed, regarding how access, authentication, and integrity were being handled in other components.

A security architecture would have allowed the designers to identify assets requiring protection. Threat modeling (See Annex B) could have been used to see how those assets could be reached. Assumptions were likely made by the different design teams that other components had security covered. For example:

- The implanted device team assumed that any command sent to the device was authorized because the range was so short. They did not consider that the range could be extended through the device accessories.

- The WCA design team assumed that the Tablet would never send unauthorized commands or firmware updates because it only connected to the company's server and used secure communications. Furthermore, it was assumed that nobody would go to the trouble to reverse engineer the WCA's firmware. They also did not realize a look-alike application could be placed on the web, and social engineering attacks could get the patient to download it. They followed the "UserID/Password" model because that is what they were accustomed to and did not realize it did not authenticate the server (only the user). They also assumed the Tablet could be trusted because it was from a major manufacturer. They did not realize that users could install malicious applications by accident.

- The Tablet team assumed that they would only communicate with the company's server and didn't realize that there were MITM attacks that could redirect their server IP address look-up to a hostile server.

The server team assumed that if they were given the correct UserID/Password, then this was an authorized user and appropriate access was provided. They assumed the Tablet would never send a command that could be harmful to the database integrity.

Design Considerations: Did you consider server attacks in your analysis? What security controls could mitigate damage from an attacker's knowledge of a UserID and Password?

The lack of a security risk analysis contributed to not knowing what should be protected. Hence, it was decided to protect everything to a convenient degree not realizing that they could not protect the entire system and their measures could be used in combination to create an effective attack.

The server was not authenticated to the user, which allowed the attacker to substitute their own server. The software and firmware downloads were also not authenticated because the designers assumed the secure communication channel would guarantee delivery of correct updates. The application was not authenticated or signed, therefore the Tablet could not distinguish it from the attacker's app.

There was incomplete application of "Least Privilege". While the server assigned roles based on UserID and Password, the In Home Monitor (IHM) was designed to send commands to the implanted device based on the programming. Only patient-safe commands were to be programmed. However, a change to the application could allow IHM to send any possible command to the device. This created a hazardous scenario when an attacker was present, while there was no such scenario with just the authorized user.

Design Considerations: Where should final authentication and authorization be performed? What is the location of the last security control before a therapy change (potentially beneficial or harmful) occurs? The importance of this question cannot be understated.

- The answer is that the final authorization is performed at the point of therapy delivery. A security risk assessment, that includes a comprehensive security architecture, would have identified hazards of allowing an untrusted device to perform any operation on the medical device. It would have shown that a system with good security practices would have classified the risks associated with each possible command, and each classification of user would only be allowed to use commands appropriate to their job.

- The analysis also would have shown that the authentication/permission process needs to be performed as close as possible to the medical therapy that could create the hazard. If it cannot be done in the implanted device, then the external accessory must be designed for security and have a robust mechanism for authenticating itself with the implanted device.

The easy availability of the app allowed the attacker to reverse engineer it and create his own app. Any secure system should not depend on hiding its design; the lack of design information increases the attacker's effort and required skill level, thus reducing the set of potential attackers.

The availability of the WCA on the used market allowed reverse engineering to extract design information required to create a modified app.

Design Considerations: Could the WCA's hardware selection provide a security control that would make reverse engineering more challenging? Security requires the combined effort of the entire design team, including electrical, mechanical, and software/firmware.

Because the attacker obtained the patient's UserID and Password, they were able to mimic the patient to the server using their own PC-based software. If they could do this for a large number of patients, they have the ability to access and modify large amounts of patient information.

Design Considerations: What security controls could be placed on the server to limit the attacker's benefit of knowing a number of UserIDs and Passwords?

E.7.3.5 Security Risk Controls

This subclause considers security risk controls that could be implemented. After implementing the controls, the security risk assessment should be updated along with the overall risk assessment as the controls have the potential to introduce or modify other safety-related risks.

a) Use two-way authentication to authenticate the Tablet application to the Server and the Server to the application. Each Tablet application installation is provided with a server (PKI) certificate that is used to authenticate the server. Similarly, the server authenticates the Tablet using the Tablet's unique certificate.

b) Implement code signing on software and firmware. Use a hash function to verify that the firmware or software is correct. The hash is signed with a private key owned by the manufacturer. The firmware and software contains the public key to verify the hash and thus verify that the update is authentic.

c) The Tablet application must perform a two-way authentication with the WCA. Each WCA is provided with a unique key or certificate known by the authorized server. The Tablet application is not allowed to communicate with the WCA or the Server until it has authenticated itself with the WCA.

d) The Tablet's application software uses a hardware key or certificate store to prevent another app from obtaining its credentials.

e) The application software is obfuscated or protected by other software to make reverse engineering more difficult. While this is not a complete solution, a difficult attack may make the product less susceptible. (The attacker will generally seek out the easiest products to attack that achieve their objective.)

f) Move safety-critical calculations and decisions to the WCA, the Server, or the Device. Reducing the capability of the Tablet app reduces the value obtained from reverse engineering.

g) Use a microprocessor on the WCA where the firmware cannot be read either through the conventional communication channels or through the processor's debugging port. Disable any debug capability that allows firmware or data to be changed via the debugging port.

h) Make it "expensive" to reverse engineer the WCA by using strong, thermally insensitive epoxies that require things to break in order to access critical electronic elements.

i) Use a secure chip to uniquely identify the WCA. This can also mitigate issues with counterfeit product.

Annex F
(informative)

A comparison of terminology between key referenced standards

The following table compares the basic terms of risk management as defined in ANSI/AAMI/ISO 14971:2007, NIST SP 800-30 Revision 1 (see Bibliography [53]), IEC 80001-1:2010 and this TIR.

Table F.1 - Related terms in security standards/technical reports

ANSI/AAMI/ISO 14971:2007	NIST SP 800-30, Rev. 1	IEC 80001-1:2010	TIR57
2.2 **harm** physical injury or damage to the health of people, or damage to property or the environment [ISO/IEC Guide 51:1999, definition 3.3]	Neither “harm” nor “impact” are defined, but a related term is “impact level” since it incorporates the term “harm”: **Impact Level** **[CNSSI No. 4009]** The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.	**2.8** **HARM** physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEM SECURITY NOTE Adapted from ISO 14971:2007, definition 2.2.	**2.11** **harm** physical injury or damage to the health of people, or damage to property or the environment, or reduction in effectiveness, or breach of data and systems security [SOURCE: IEC 80001-1:2010, definition 2.8]

ANSI/AAMI/ISO 14971:2007	NIST SP 800-30, Rev. 1	IEC 80001-1:2010	TIR57
2.3 **hazard** potential source of harm [ISO/IEC Guide 51:1999, definition 3.5] NOTE, Annex E in ISO 14971 states "According to the definitions, a hazard cannot result in harm until such time as a sequence of events or other circumstances (including normal use) lead to a hazardous situation."	The term "hazard" is not defined or used in the document. A "vulnerability" is generally considered to be a specific type of hazard: **Vulnerability** **[CNSSI No. 4009]** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.	The term "vulnerability" is not defined or used in the document. The definition of "hazard" is identical to that contained in ISO 14971 but includes the expanded definition of "harm": **2.9** **HAZARD** potential source of HARM [ISO 14971:2007, definition 2.3]	Both "hazard" and "vulnerability" (a specific type of hazard) are defined in TIR-57. The definition of "hazard" is identical to that contained in ISO 14971 but includes the expanded definition of "harm": **2.12** **hazard** potential source of harm [SOURCE: ISO/IEC Guide 51:1999, definition 3.5] **2.35** **vulnerability** weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200]
2.4 **hazardous situation** circumstance in which people, property, or the environment are exposed to one or more hazard(s) [ISO/IEC Guide 51:1999, definition 3.6] NOTE See Annex E for an explanation of the relationship between "hazard" and "hazardous situation."	The term "hazardous situation" is not defined. A "threat event" is generally considered to be a specific type of hazardous situation: **Threat Event** An event or situation that has the potential for causing undesirable consequences or impact.	The document includes several instances of the term "hazardous situation" but it is not defined. The term "threat event" is not defined but the term "threat(s)" is used in two instances.	Both "hazardous situation" and "threat event" are defined in TIR-57: **2.13** **hazardous situation** circumstance in which people, property, or the environment are exposed to one or more hazard(s) NOTE 1 to entry: See Annex E, ANSI/AAMI/ISO 14971:2007, for an explanation of the relationship between "hazard" and "hazardous situation". **2.32** **threat event** event or situation that has the potential for causing undesirable consequences or impact [SOURCE: SP 800-30]

ANSI/AAMI/ISO 14971:2007	NIST SP 800-30, Rev. 1	IEC 80001-1:2010	TIR57
Probability of occurrence of harm Although not a defined term, this factor is included in the definition of "risk" and is further elaborated in Annex E: Probability of occurrence of harm = P1 x P2 P1 is the probability of a hazardous situation occurring. P2 is the probability of a hazardous situation leading to harm.	**Likelihood of Occurrence [CNSSI No. 4009, adapted]** A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.	The phrase "probability of occurrence of harm" (Annex E, ISO 14971) is included in the definition of "risk".	The phrase "probability of occurrence of harm" (Annex E, ISO 14971) is included in the definition of "risk". TIR-57 also defines the term "likelihood of occurrence" based on CNSSI-4009 but adds an informative note that includes the term "threat event": **2.16** **likelihood of occurrence** weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. NOTE 1 to entry: Likelihood of occurrence combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts). [SOURCE: CNSSI-4009, modified - the phrase "In Information Assurance risk analysis," was removed.]
The definition of "risk" includes the factor "probability of occurrence": **2.16** **risk** combination of the probability of occurrence of harm and the severity of that harm [ISO/IEC Guide 51:1999, definition 3.2]	The definition of "risk" includes the factor "likelihood of occurrence": **Risk** **[CNSSI No. 4009]** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. See Information System-Related Security Risk.	The definition of "risk" is identical to that contained in ISO 14971 but includes the expanded definition of "harm": **2.23** **RISK** combination of the probability of occurrence of HARM and the severity of that HARM [ISO 14971:2007, definition 2.16]	The definition of "risk" is identical to that contained in ISO 14971 but includes the expanded definition of "harm": **2.23** **risk** combination of the probability of occurrence of harm and the severity of that harm [SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Bibliography

[1] ANSI/AAMI ES60601-1:2005(R) 2012, *Medical electrical equipment - Part 1: General requirements for basic safety and essential performance.* Association for the Advancement of Medical Instrumentation;2005(R)2012. Arlington, VA.

[2] ANSI/AAMI/ISO 14971:2007, *Medical devices - Application of risk management to medical devices.* Association for the Advancement of Medical Instrumentation;2007. Arlington, VA.

[3] ANSI/AAMI/ISO TIR24971:2013, *Guidance on the application of ISO 14971.* Association for the Advancement of Medical Instrumentation;2013. Arlington, VA.

[4] ANSI/AAMI/IEC 62366-1:2015, *Medical devices - Part 1: Application of usability engineering to medical devices.* Association for the Advancement of Medical Instrumentation;2015. Arlington, VA.

[5] ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT networks incorporating medical devices - Part 1: Roles, responsibilities and activities*. Association for the Advancement of Medical Instrumentation;2010. Arlington, VA.

[6] AAMI/ANSI/IEC, TIR 80001-2-2:2012, *Application of risk management for IT networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*. Association for the Advancement of Medical Instrumentation;2012. Arlington, VA.

[7] AbuLamddi M. Security engineering methods and approaches used in SDLC. *International Journal of Research in Engineering & Applied Sciences*. 2013:(6).

[8] Anderson RJ. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley; 2008.

[9] Ashbaugh D. *Security Software Development, Assessing and Managing Security Risks*. CRC Press. Boca Raton, FL: Auerbach Publications: 2009.

[10] Axelrod CW. *Engineering Safe and Secure Software Systems*. Norwood, MA: Artech House; 2013.

[11] Bishop M. *Computer Security: Art and Science*. Indianapolis, IN; Addison-Wesley Professional; 2002.

[12] Bistarelli S, Peretti P, & Trubitsyna I. *Defense trees for economic evaluation of security investments*. Informally published manuscript, Department of Mathematics and Computer Science, University of Perugia, Perugia, Italy. 2006.

[13] Bode S, Fischer A, Kunhauser W, Riebisch M. *Software Architectural Design Meets Security Engineering*, 16th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems. 2009.

[14] Cebula J, Young L. (2010) *A Taxonomy of Operational Cyber Security Risks*. Carnegie Mellon Software Engineering Institute Technical Note. http://www.sei.cmu.edu/reports/10tn028.pdf

[15] Center for Internet Security (CIS), *Cyber Hygiene Toolkit*, https://www.cisecurity.org/cyber-pledge/tools/ (Accessed January 12, 2016)

[16] Committee on National Security Systems (CNSS) Instruction No.4009, *National Information Assurance (IA) Glossary*, June 2006. http://jitc.fhu.disa.mil/pki/documents/committee_on_national_security_systems_instructions_4009_june_2006.pdf (Accessed 10 January 2016)

[17] FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf (Accessed 10 January 2016)

[18] Defense Acquisition Guidebook: https://acc.dau.mil/CommunityBrowser.aspx?id=492083

[19] Defense Technical Information Center: *Resilient Military Systems and the Advanced Cyber Threat* - Defense Science Board, January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf (Accessed 10 January 2016)

[20] D Edge KS. *A framework for analyzing and mitigating the vulnerabilities of complex systems via attack and protection trees*. (Doctoral dissertation). 2007.

[21] FIPS 140-2:2001, *Security Requirements for Cryptographic Modules*

[22] FIPS 185:1994, *Escrowed Encryption Standard*

[23] FIPS 199:2004, *Standards for Security Categorization of Federal Information and Information Systems*

[24] FIPS 200:2006, *Minimum Security Requirements for Federal Information and Information Systems*

[25] Forum of Incident Response and Security Teams. *Common Vulnerability Scoring System (CVSS)*. https://www.first.org/cvss (Accessed on June 15, 2015.)

[26] Garzia VF, Brebbia CA, Guarascio M. *Safety and Security Engineering*, WIT Press; 2013.

[27] Gollmann D. *Computer Security*. Hoboken, NJ: Wiley; 2011.

[28] HIMSS/NEMA Standard HN-1:2013, *Manufacturer Disclosure Statement for Medical Device Security (MDS2)*.

[29] Howard M, LeBlanc D. *Writing Secure Code.* Microsoft Press. 2nd ed.; 2002.

[30] IEC/TS 62443-1-1 Edition 1.0 2009-07, *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*.

[31] IEC 62443-2-1 Edition 1.0 2010-11, *Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program*

[32] IEC/TR 62443-3-1 Edition 1.0 2009-07, *Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems*.

[33] IEC 62443-3-3:2013, *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

[34] IEC/TR80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the communication of medical device security needs, risks and controls*

[35] IEC DTR80001-2-8 (Draft), *Application of risk management for IT-networks incorporating medical devices Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2.*

[36] Internet Security Alliance, *Sophisticated Management of Cyber Risk: Maintaining Focus on Good Cyber Hygiene*; 2013.

[37] IEEE Center for Secure Design, *Avoiding the Top 10 Software Security Design Flaws*, 12 November 2015, http://cybersecurity.ieee.org/2015/11/13/avoiding-the-top-10-security-flaws/ (Accessed 10 January 2016)

[38] ISO/IEC Guide 51:1999, *Safety aspects — Guidelines for their inclusion in standards*

[39] ISO/IEC 29147:2014, *Information technology – Security techniques – Vulnerability disclosure*

[40] ISO/IEC 30111:2013, *Information technology – Security techniques – Vulnerability handling processes*

[41] ISO 9000:2005, *Quality management systems -- Fundamentals and vocabulary*

[42] ISO 27005, *Information technology - Security techniques - Information security risk management*

[43] Kleidermacher D, Kleidermacher M. *Embedded Systems Security*. Oxford, UK: Elsevier; 2012.

[44] McDermott J, Fox C. (Dec 1999). *Using Abuse Case Models for Security Requirements Analysis*. Proceedings of the 15th Annual Computer Security Applications Conference. 1999:55–64.

[45] McGraw G. *Software Security: Building Security In*. Boston, MA: Pearson Education; 2006.

[46] MITRE. *Common Attack Pattern Enumeration and Classification (CAPEC)* https://capec.mitre.org/ (Accessed on January 7, 2016).

[47] MITRE. *Common Vulnerabilities and Exposures (CVE).* https://cve.mitre.org/ (Accessed on June 15, 2015.)

[48] MITRE. *Common Weakness Enumeration (CWE).* https://cwe.mitre.org/ (Accessed on June 15, 2015.)

[49] NASA. *Systems Engineering Handbook*. SP-610S. June 1995.

[50] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*; Version 1.0, February 12, 2014.

[51] NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*

[52] NIST SP 800-27A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*

[53] NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessment*

[54] NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

[55] NIST SP 800-39, *Managing Information Security Risk*.

[56] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

[57] NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*

[58] NIST SP 800-70 Rev. 3, *National Checklist Program for All IT Products-Guidelines for Checklist Users and Developers*

[59] NIST SP 800-60 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*

[60] NIST SP 800-92, *Guide to Computer Security Log Management.*

[61] NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*

[62] NIST SP 800-118, *DRAFT Guide to Enterprise Password Management*

[63] NIST SP 800-160, *Systems Security Engineering – An Integrated Approach to Building Trustworthy Resilient Systems.*

[64] *Open Security Architecture*. (n.d.). Retrieved from http://www.opensecurityarchitecture.org/cms/

[65] Open Web Application Security Project (OWASP). *OWASP Risk Rating Methodology* https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (Accessed on June 15, 2015.)

[66] Pfleeger C, Pfleeger S. *Security in Computing. 4th edition*. Prentice Hall; 2012.

[67] Roy A. *Attack countermeasure trees: A non-state-space approach towards analyzing security and finding optimal countermeasure sets*. (Master's thesis). 2010.

[68] Rozanski N, Woods E. *Software Systems Architecture: Working With Stakeholders Using Viewpoints and Perspectives. 2nd Ed*. Indianapolis, IN: Addison-Wesley Professional. 2011.

[69] Saltzer J, Schroeder M. Principles for Information Security Protection. *Proceedings of the IEEE.* 1975; 63(9)*;*1278-1308.

[70] SANS Institute (2007), *Software Engineering – Security as a Process in the SDLC*: http://www.sans.org/reading-room/whitepapers/securecode/software-engineering-security-process-sdlc-1846

[71] Schneier B. *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ: Wiley; 2004.

[72] Stallings W, Brown L. *Computer Security, Principles and Practice. 2nd ed*. Prentice Hall; 2012

[73] United States Computer Emergency Readiness Team (US-CERT). https://www.us-cert.gov/ (Accessed on January 7, 2016.)

[74] U.S. Department of Health & Human Services, *HIPAA Administrative Simplification Regulations, 45 CFR Part 160, Part 162, and Part 164*; 2013.

[75] U.S Government Printing Office, 44 U.S. Code § 3542*, Title 44 – Public Printing and Documents, , Chapter 35 – Coordination of Federal Information Policy, Subchapter III – Information Security, Sec. 3542 - Definitions*