Cybersecurity for medical devices: recommended best practices during design, development and deployment

Bernhardt, Richard; Jiang, Di; D'amours, Danny; Glasgow, Ian; White, Debbie; Clark, Cory

https://doi.org/10.4224/40000465

NRC·CNRC

Cybersecurity for Medical Devices: Recommended Best Practices During Design, Development and Deployment

Report No: 2019-003
Date: May 2019
Authors: Richard Bernhardt, NRC
Di Jiang, NRC
Danny D'Amours, NRC
Ian Glasgow, Health Canada
Debbie White, Canadian Centre for Cybersecurity
Cory Clark, Canadian Centre for Cybersecurity

Medical Devices Research Centre

National Research Council Canada
Conseil national de recherches Canada

Canada

Disclaimer

The advice given and opinions expressed herein are supplied on an “as is” basis.

There are no representations or warranties with respect to fitness for any use or purpose, quality, or freedom from defects or inaccuracy of advice given or opinions expressed.

NRC rejects all liability and responsibility relating to the consequences of using the information in this document.

Revision History

Date	Changes
Jun 2019	Initial Issue

Cat. No. NR16-286/2019E-PDF
ISBN 978-0-660-31844-5

Contents

List of Tables

List of Figures

1 Introduction

The digital revolution that resulted in the development of the Internet and connected devices such as smartphones is beginning to permeate the health care environment, with the promise of empowered patients, better diagnoses and lower costs [1]. This revolution is expected to result in an increase in the number of connected medical devices. Some of these new medical devices may appear unconventional, without any obvious patient interaction; some may consist solely of software running on General Purpose Computers (GPCs) or on mobile devices. Therapies using smartphone apps have even supplanted pharmaceuticals in some cases [2]. Unfortunately, with this promise comes the possibility of cyberattacks and intrusions against a compromised connected medical device, and the network to which such a device is connected.

Fortunately, as of the date of publication of this report, there have been no verified accounts of a compromised connected medical device resulting in patient harm [3]. However, there have been incidents of cyberattacks seriously impacting healthcare organizations; perhaps the most notable example is the May 2017 WannaCry ransomware attack and its effect on Britain's National Health Service. The attack resulted in hospitals locked out of their information technology (IT) systems, doctors unable to call up patient records and emergency rooms forced to divert people seeking urgent care [4][1]. This was an example of the consequences of a successful cyberattack on a health care organization. Overall, the number of cyberattacks per year is increasing, with the cost to the attacked organization in the millions of dollars in some cases [5, p. 9].

The consequences of these attacks, and the corresponding costs that can result from them, have prompted many governments to undertake measures to protect themselves and their citizens [6] [7] [8]. These measures have come not only from those government agencies with specific responsibility for cybersecurity, but also from agencies with an interest in the impact of cybersecurity on their areas of responsibility. Beside government agencies, other entities, such as businesses, industry associations, technical societies, standards organizations, universities, research institutions, policy groups and non-governmental organizations, covering a broad range of activities, including health care and medical devices, have also taken an interest in cybersecurity issues.

The health care field, and within it, connected medical devices, has proven to be a valuable target for cyber threat actors (more commonly known as hackers) for the following reasons [9]:

1. Compromised patient data, particularly past test results, cannot be recreated easily, if at all. Additionally, patient data may have other non-medical attributes such as Personally Identifiable Information (PII)[2] that are desirable to criminal elements.

[1] The United Kingdom National Audit Office believes 19,000 appointments had to be cancelled. [84]
[2] Social Security numbers in the United States are particularly prized.

2. Medical devices tend to have long service lives; therefore legacy devices may lack the ability to be updated with the latest cybersecurity software.
3. Physical access to hospitals is at best loosely controlled. Furthermore, many connected medical devices are located in public areas of the hospital. This allows threat actors potential physical access to connected equipment.
4. Hospitals in Canada may face budget limitations when attempting to keep up with the latest cybersecurity practices.
5. Many of these new devices are expected to move into the home, which is even more uncontrolled than a hospital.
6. The increased connectivity of medical devices makes them vulnerable to unauthorized access and exploitation.

Because of these factors, government agencies responsible for the regulation of medical devices (such as Health Canada and the US Food and Drug Administration (FDA)) have turned their attention to improving the cybersecurity of these devices. These agencies have been assisted by various other interested organizations.

1.1 Relevant Government Stakeholders

1.1.1 Health Canada

Within Canada, Health Canada is the federal government department responsible for the regulation and licensing of medical devices. Recognizing the need to support the fast pace of the digitally-driven evolution of medical devices, in March 2018 the department established the Digital Health Review Division within the Medical Devices Bureau [10]. As part of this initiative, Health Canada also established a Scientific Advisory Committee on Digital Health Technology (SAC-DHT) to provide timely advice on a variety of issues related to digital technology in medical devices, including cybersecurity [11]. The first meeting of the SAC-DHT took place on November 23, 2018 with medical device cybersecurity as its primary focus [12]. As part of this meeting, the SAC-DHT considered a Health Canada document, “Draft Guidance Document – Pre-market Requirements for Medical Device Cybersecurity” [13], which was released for public comment following the meeting. This guidance document is examined as part of this report (see section 6).

1.1.2 Communications Security Establishment

The Communications Security Establishment (CSE) is the federal government agency with primary responsibility for cybersecurity. One of its main roles is to help ensure the protection of electronic information and information infrastructure that are important to Canada [14]. Most of this activity has focused on federal government information and related infrastructure. However, in recognition of the increasing importance of cybersecurity to all Canadians, the CSE role was expanded by the creation of the Canadian Centre for Cyber Security [6]. One of the Cyber Centre’s roles is to certify IT products to various recognized specifications and standards including the Common Criteria (CC) [15], which is an internationally recognized standard built upon specifications called Protection Profiles (PPs). These PPs can be leveraged by medical device developers as described in sections 5.1.3, 7.1, 7.3.2 and 9.4.1.

1.1.3 National Research Council

The National Research Council (NRC) is the largest research organization within the Government of Canada, with a variety of activities and interests, including medical device research and development. The NRC has a history of developing innovative medical devices, including one of the first cardiac pacemakers and the first useable motorized wheelchair [16].

The NRC has three mandates: support policy; spur business innovation; and generate knowledge. Via these mandates, and the resulting interactions with industry and with the rest of government, the NRC has a good understanding of industry needs for rapid rates of innovation, as well as government needs for maximizing public safety.

The NRC Medical Devices Research Centre has an appreciation of the challenges confronting medical device manufacturers, which now include cybersecurity.

2 Abbreviations and Definitions

2.1 Abbreviations

AAMI – Association for the Advancement of Medical Instrumentation
APT – Advanced Persistent Threat
ANSI – American National Standards Institute
BOM – Bill of Materials
CC – Common Criteria
CCCS – Canadian Centre for Cybersecurity
CCTX – Canadian Cyber Threat Exchange
CoP – Code of Practice
COTS – Commercial off-the-shelf
CSA – Canadian Standards Association
CSE – Communications Security Establishment
CWE – Common Weakness Enumeration
CVE – Common Vulnerabilities and Exposures
CVP – Cyber Verification Program
CVSS – Common Vulnerability Scoring System
EHR – Electronic Health Record
GSR – Galvanic Skin Resistance
HSCC – Healthcare and Public Health Sector Coordinating Council
ISAC – Information Sharing and Analysis Centre
ISAO – Information Sharing and Analysis Organization
IEC – International Electrotechnical Commission
IoT – Internet of Things
IoMT – Internet of Medical Things
ISO – International Standards Organization
JSP – Joint Security Plan
NCCoE – National Cybersecurity Center of Excellence
NIST – National Institute of Standards and Technology
NVD – National Vulnerability Database

OWASP – Open Web Application Security Project
PETRAS – Privacy, Ethics, Trust, Reliability, Acceptability and Security
PII – Personally Identifiable Information
PP – Protection Profile
PPG – Photoplethysmograms
RPM – Remote Patient Monitoring
SME – Subject Matter Expert
TIR – Technical Information Report
UL – Underwriters Laboratories

2.2 Definitions

For this document, and in the context of a medical device, the following definitions apply:

attack – a realized threat, usually but not necessarily overt (that is, the victim realizes that they have been attacked); synonymous with cyberattack

cybersecurity - the body of technologies, processes, practices, responses and mitigation measures designed to protect a medical device against unauthorized access, modification, misuse, or denial-of-use, and against the unauthorized use of information associated with a medical device

event – an attack or intrusion; synonymous with cybersecurity event

hactivist – a threat actor with social or political motivations

intrusion – a realized threat, necessarily covert (that is, the victim is unaware of the intrusion); synonymous with cyberintrusion

malware - software designed with malicious intent to disrupt normal function, gather sensitive information, and/or access other connected systems

threat - any circumstance or event with the potential to adversely impact health and safety via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

threat actor – individual, group, organization or government that conducts or has the intent to conduct detrimental activities; synonymous with attacker and hacker

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

3 Purpose

The purpose of this report is to describe cybersecurity-related best practices for medical device developers to consider during the pre-market design and development phases. Several recommendations also are relevant to post market surveillance activities. The report is meant to complement the Health Canada pre-market guidance document introduced in section 1.1.1 and discussed in section 6. This document will provide additional insight, information and hints that developers of medical devices can leverage in their activities. It will also provide a worked example that developers can use as a starting point in their efforts.

3.1 Scope

The focus of this report is to describe best practices for incorporating cybersecurity into medical devices, including aspects specific to Canada[3]. Non-cybersecurity related aspects of medical device design and development, such as developing software, performing a safety risk analysis or instituting a quality system are not covered, except when these intersect with cybersecurity related concerns. Information related to these topics can be found from a variety of sources, in particular IEC 62304 for software development [17], ISO 14971 for safety risk analysis [18] and ISO 13485 for quality system implementation [19].

There are several "best cybersecurity practices" documents prepared by a number of different organizations, including standards organizations [20], technical societies [21] and businesses [22]. Their focus may be specific to medical devices, but some are on related subjects, such as the Internet of Things (IoT)[4]. Most provide useful information; several will be examined more closely in this report. However, much of the information tends to be fairly general or high-level. Moreover, application of the information may not be obvious, particularly to developers with limited cybersecurity experience. As a contrast to this trend, in addition to reiterating general information, a system currently being developed by the Simulation and Digital Health (S&DH) Section of the NRC Medical Devices Research Centre (bConnected) will be examined in this report and used to illustrate more concretely the application of these "best cybersecurity practices" (see section 9).

A deconstruction of a specific application is not unique to this report. Appendix E of the Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report (TIR) 57:2016 [21] uses a fictional system, the "Kidneato artificial implantable kidney", for a similar purpose. Additionally, the US National Institute for Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) has announced that they will prepare a cybersecure TeleHealth Remote Patient Monitoring (RPM) reference design [23].

---

[3] One challenge for medical device companies entering the Canadian market is the federal/provincial division of responsibilities for certain aspects of medical device cybersecurity. For example, a cybersecurity vulnerability that could result in a breach of patient health information but have no impact on patient safety may not fall under the authority of Health Canada. However it may fall under other provincial or federal legislation.

[4] IoT refers to the technological development whereby all manner of devices (ex. home thermostats, traffic control lights, transit buses) are connected to the Internet, usually wirelessly. Connected medical devices can be considered the Internet of Medical Things (IoMT), a subset of the IoT.

3.2 Intended Audience

The intended audience for this report is a medical device designer and developer with hitherto limited exposure to and experience with cybersecurity design practices and considerations. Those developers with more cybersecurity experience and exposure may also find this report beneficial. Individuals responsible for cybersecurity in a hospital or clinic may also gain some insight into medical device cybersecurity, as could individuals concerned about the security of medical devices in their homes.

3.2.1 Assumptions

It is assumed that a designer and developer who wishes to learn more about cybersecurity for medical devices is familiar with many of the medical device regulatory standards. In particular, it is assumed that the designer/developer's organization has instituted, or is in the process of instituting, a quality system in accordance with ISO 13485:2016, has the appropriate software design controls in place to meet IEC 62304:2015, and has initiated a safety risk analysis in accordance with ISO 14971:2007. Designers unfamiliar with these standards should review them, particularly IEC 62304 and ISO 14971 as they are recognized standards by Health Canada and constitute best design practices. Health Canada also has an e-Learning tool, "How Medical Devices Are Regulated in Canada"[5] that is useful for developers looking for more background information on this subject.

Recommendation

Review ISO 14971:2007 and IEC 62304:2015

4 The Essence and Infrastructure of Cybersecurity

There is a wealth of information on all aspects of cybersecurity available from a wide variety of sources [9], [21], [22], [24]. Much of it is based upon a few common concepts, some of which are summarized here.

4.1 The C-I-A Triad

In the cybersecurity world, the term "C-I-A" or "C-I-A triad" refers to:

1. Confidentiality – means that unauthorized individuals cannot access information that involved parties wish to remain confidential. So, if the information is stored on a computing device (also known as information-at-rest), then only authorized users are permitted access. The information could be stored unencrypted (plaintext) or encrypted. If the information is transmitted electronically (data-in-motion), then this information is encrypted so that, if it is intercepted, it will be meaningless to unauthorized recipients.
2. Integrity – means that information is protected from being modified or deleted by unauthorized parties. Thus, a recipient or user of information can be certain that

[5] https://training-formation.phac-aspc.gc.ca/course/index.php?categoryid=42&lang=en

the information is accurate and uncorrupted. It also means that the sender or holder of the information cannot repudiate what was transmitted, or made available to others. The users of the information can trust it. For a medical device, integrity can also mean that the device itself functions in accordance with its intended use.

3. Availability – in a general cybersecurity sense, this means that information can be accessed by authorized users when it is needed. For a medical device, this can also mean that either the information, or the device itself, is able to be used by an authorized user when it is required.

The C-I-A triad has a different weighting for medical devices than the traditional application of the triad to IT security as breaches in integrity and availability may have a greater impact on patient safety.

Other terms frequently associated with these three are authentication, authorization and access control. Authentication is the process of verifying the identity of a party requesting information, service or use of a device. Authorization is the process of granting an authenticated party access to the requested information, service or use of the device. Access control is the process by which an authenticated, authorized party is only allowed access to certain information, services or devices. An authenticated party may have no authorization to access any information, service or device.

One specific type of authentication is mutual authentication, or two-way authentication, whereby two parties in an exchange authenticate each other at the same time. This is not the default in all communications protocols. In a medical device, performing mutual authentication is particularly important if a change to a device setting or the software itself is commanded remotely (see section 9.3.3).

Recommendation

Perform mutual authentication for any remotely commanded setting change

4.2 Cryptography, Keys and PKI

As was noted in section 4.1, the use of encryption for protecting information is ubiquitous. Cryptography is the scientific discipline that ensures secure communication between two parties in the presence of a third party who should not be privy to their communication [25]. It relies heavily on mathematical algorithms that perform the actual encryption. To be useful, these algorithms need keys, which in a digital computer, are strings of bits that are combined mathematically with the information to be protected. Only those individuals that possess the key will be able to decrypt the protected information. This arrangement, whereby both parties to a secure exchange of information use the same key, is called symmetric-key cryptography.

The symmetric-key method or secret key cryptography is impossible to use if the two parties who wish to communicate securely do not hold the same key. In this case, a different cryptographic method, called asymmetric-key cryptography or public key cryptography is used. In this situation, each party possesses a pair of keys, called the public/private key pair. The key pair is related mathematically. The public key is available

to anyone. It is used to encrypt a message which can then only be decrypted by the associated private key. For obvious reasons, the private key must be kept strictly confidential. For this method to work, some way of validating that a public key belongs to a particular party is needed. The infrastructure needed to create this validation is called the Public Key Infrastructure (PKI). Further information on PKI can be found in a variety of references; Chapter 18 of [26] is particularly informative and readable.

The algorithms used for encryption/decryption are known, unsurprisingly, as cryptographic algorithms. Two widely used ones are AES (Advanced Encryption Standard) [27] originally known as Rijndael, and RSA (Rivest-Shamir-Adelman) [28]. AES is a symmetric key algorithm, while RSA is an asymmetric key one. When use of a cryptographic algorithm is specified the key length is specified as well. So for example AES-256 means the AES algorithm employing a 256 bit key. Typical AES key lengths are 128, 192 and 256 bits, while those for RSA are 1024, 2048 and 3072. Larger keys result in more secure messages, with a penalty of increased computation time. Note that the same key length for one algorithm does not result in the same level of security when used with another algorithm. So for example, a 3072 bit RSA key is equivalent in strength to a 128 bit symmetric key [29].

Due to the length of the keys, and the nature of the algorithms, asymmetric encryption is slower than symmetric encryption; therefore use of symmetric encryption is naturally favored but as noted earlier requires both parties to have possession of the same key. In many cases therefore a secure exchange begins by using the PKI and asymmetric algorithms to exchange a symmetric key.

The invention of highly secure cryptographic algorithms and their proper implementation are best left to Subject Matter Experts (SMEs). To give an indication of the serious nature of such an undertaking, the CSE, jointly with NIST, manages two cryptographic quality assurance programs, the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CAVP) [30] for validating algorithms and their implementation. These programs are similar in nature to the Common Criteria program mentioned in section 1.1.2 and described elsewhere in this report. Medical device developers should not undertake the development of their own cryptographic algorithms and modules. Instead, they should use the latest version of those algorithms recognized as best in class.

Recommendations

Use widely accepted cryptographic algorithms

Do **NOT** develop custom cryptographic algorithms and implementations

4.3 Threat Actors

By definition, threat actors are individuals, groups, organizations or governments that conduct or have the intent to conduct detrimental activities. The more common term is hacker. The CSE classifies threat actors by their motivation and, to a lesser extent, their sophistication [31]. Their classification scheme is shown in Table 1.

Threat Actor	Motivation	Sophistication
Nation-states	Geopolitical	Very high[1]
Cybercriminals	Profit	High[2]
Hacktivists	Ideology	Low to moderate
Terrorist Groups	Violent ideology	Low to moderate
Thrill-seekers[3]	Psychological	Low
Insiders	Discontentment	Not applicable

Notes:
1. Nation state threat actors are generally well funded with highly trained and well managed personnel.
2. Cybercriminals are less sophisticated than nation states but usually have better capabilities than the less sophisticated threat actors.
3. Other common terms for threat actors in this class are hackers and script-kiddies

Table 1: Threat Actor Classification

Well-resourced, sophisticated threat actors are often referred to as Advanced Persistent Threats (APTs). As the term suggests, APTs are not deterred by the most common cyber defenses and will probably be able to overcome those measures put in place by most medical device developers. However, using the best practices described or pointed to in this report will frustrate the less sophisticated threat actors to such a degree that they will look elsewhere to attack.

4.4 Types of Attacks

The Wanna Cry cyberattack mentioned in section 1 was a ransomware attack in which malware surreptitiously installed on a computer encrypts the hard drive, rendering it unusable, and demands a ransom to return the drive to its unencrypted state. There are many different types of attacks, some of which are listed here:

1. Eavesdropping – a threat actor monitors a communication channel for messages, without modifying the message.
2. Man-in-the-middle (MiTM) – by masquerading as the bona-fide receiver of a message, a threat actor intercepts the message and modifies it before sending it to the intended recipient.
3. Password compromise – ranges from brute force guessing to use of a compromised password hash (basically an encrypted password) to gain unauthorized access to a device and/or network.
4. Denial of Service (DoS) – by using a network of compromised computers, a server is inundated with bogus requests for service which denies service to legitimate requests.
5. Update Compromise - threat actors may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the

device. Non-validated updates or updates validated using non-secure or weak cryptography leave the updated firmware vulnerable to surreptitious alteration.

Some degree of familiarity with the various types of attacks is helpful, as a developer will have to perform specific tests to show that their design is secure against specific attacks (see section 7.3).

4.5 Vulnerabilities and Vulnerability Databases

Simply put, a vulnerability is a weakness that can be exploited by a threat actor to launch an event. Most exploits are made possible by the existence of old vulnerabilities for which solutions (usually a software patch) exist [24]. There are more than 100000 known vulnerabilities cataloged in two databases called the Common Vulnerabilities and Exposures (CVE) [32] and the National Vulnerability Database (NVD) [33]. Mitre Corporation maintains the CVE catalog as a contractor to the US government, while the NVD is maintained by NIST. Both databases are publicly available on the internet. In addition to known vulnerabilities, there are also zero-day vulnerabilities or exploits, which are newly discovered vulnerabilities for which there are no fixes.

Related to the vulnerability catalogs is the Common Weakness Enumeration (CWE) [34]. It is also maintained by Mitre. The CWE is a dictionary of common software weaknesses or errors that can result in vulnerabilities. Developers can analyze their code using the information found in the CWE. The CWE is publicly available on the internet.

Also related to the vulnerability catalogs and the CWE is the Common Vulnerability Scoring System (CVSS) [35] . The CVSS employs a standardized method to indicate the severity of a vulnerability by producing a numerical score. It is maintained by the First Special Interest Group. The CVSS is also publicly available on the internet.

The CVE and NVD databases should be examined during device development to see if a particular design choice has a known vulnerability. An incident reported in the medical device cybersecurity press illustrates the reason for this activity [36]. A cybersecurity researcher reported a vulnerability in a medical gateway device, prompting an advisory from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [37]. The vulnerability is known as the “Misfortune Cookie” and has CVE catalog numbers of CVE-2014-9222 [38] and -9223 [39]. The developer of the software used in the device had originally identified the problem in 2005 and provided a fix at that time [40]. However, other manufacturers continued to use the flawed code, even though the problem had been known for over a decade. This vulnerability was given a CVSS score of 9.8 out of 10, which is considered critical. Consulting the CVE and NVD databases during testing is a recommendation of the Health Canada Pre-market Guidance document [13], as is use of the CWE.

Recommendation

Refer to the vulnerability databases frequently in both the pre- and post-market phases of the medical device lifecycle

4.6 ISACs and ISAOs

ISAC stands for Information Sharing and Analysis Center, while ISAO stands for Information Sharing and Analysis Organization. ISACs and ISAOs share information on cybersecurity risks and incidents. ISACs are predominantly involved with critical infrastructure, while ISAOs are not affiliated with a particular sector. Both types are facilitated by various agencies of the US government. In the US, medical device manufacturers are encouraged to join an ISAO. The H-ISAC has medical device manufacturers as members [41]. The Canadian Cyber Threat Exchange (CCTX) [42] is Canada's only cyber threat collaboration forum, and, while not focusing exclusively on medical devices, does have a health care component. Membership of an appropriate ISAO or ISAC is also encouraged in Canada, although not specifically required by Health Canada. However, membership will help with pre- and post- market surveillance activities and does demonstrate a commitment to ongoing maintenance.

Recommendation

Consider joining an ISAC/ISAO

4.7 Cybersecurity Frameworks

As part of its efforts related to cybersecurity, NIST has developed a set of "standards, guidelines and best practices to manage cybersecurity risk" [43] that is referred to as the Framework. It originally focused on critical infrastructure (for example, telecommunications, transportation (road/rail/aircraft), energy (pipelines, power grids)) but due to its utility, other fields adopted it. Health Canada recommends that medical device manufacturers leverage the NIST Framework in their operations (see Appendix A of the Pre-market Guidance document [13]). The US Food and Drug Administration has a similar recommendation [44].

A similar framework, ITSG-33 [45] has been developed by the CSE and reflects the same risk management approach as the NIST Framework.

Employing a framework can help to instill a culture of cybersecurity awareness in an organization in much the same way that employing ISO 13485 can instill a culture of quality [46].

Recommendation

Become familiar with a cybersecurity framework

5 Standards, Reports and Related Resources

> "When you have hundreds and hundreds and hundreds of really fine standards in a sector, guess what. You don't have any standard. We have too many standards"[6]

As mentioned in section 3.1, there are a large number of available best practices documents along with many standards, guidance documents, technical society publications and the like. This large volume of reference material can be both a blessing and a curse. It is a blessing as a neophyte has plenty of material with which to increase their knowledge of cybersecurity. It is a curse as the sheer volume of seemingly relevant and important material can consume an inordinate amount of time to review. With this in mind, several of the most pertinent references are examined here. Table 2 provides a brief overview of each.

Number/Title	Summary	Section
UL2900-1,-2-1	Two part National Standard addressing risk management and testing. Referenced in Health Canada's Premarket Guidance Document	5.1.1
AAMI TIR57	Nominally addresses risk but contains additional valuable information on a number of topics. Its detailed risk analyses may serve as a starting point for a medical device developer. Also referenced in Health Canada's Premarket Guidance	5.1.2
Common Criteria	Cybersecurity quality assurance program with associated specifications, many of which can be leveraged by developers	5.1.3
IEC 80001	Series of standards discussing incorporation of connected medical devices into a clinical IT network, such as a hospital	5.1.4
UL IoT Top 20	IoT security requirements that can be considered during cybersecurity requirement formulation	5.2.1
UK Government Secure by Design	Includes Code of Practice that can be adapted by medical device developers	5.2.2

[6] Brian Fitzgerald, Senior Technical Manager, Office of Science and Engineering, Center for Device and Radiological Health, US Food and Drug Administration, stated during Plenary Panel IX, FDA Public Workshop – Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, January 29-30, 2019 [79]

Petras Summary	UK universities consortium overview of principles and practices for IoT security that can be adopted by medical device developers	5.2.3
BSI white paper	Discusses the dichotomy between risk analysis for medical device safety versus medical device cybersecurity	5.2.4
Joint Security Plan	A total product lifecycle reference guide for developing, and deploying, cyber secure technology solutions in the health care environment	5.2.5
NIST Reference Designs	Like TIR57, contains very detailed risk analyses that may serve as a starting point for a medical device developer	5.3.1
OWASP	Testing Guide contains very detailed test instructions for web applications. Also discusses requirements, threat modeling and a cybersecurity framework	5.3.2
CSA CVP	Standard under development that will consider product and organization cybersecurity readiness	5.3.3

Table 2: Standard, Report and Related Resource Summary

5.1 Standards

5.1.1 UL 2900

UL 2900-1, “Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements” [47] and its companion document, UL 2900-2-1 “Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems” [48] are standards developed by Underwriters Laboratories. UL 2900-1 is a joint Canada-United States National Standard while UL 2900-2-1 is an American National Standards Institute (ANSI) standard. The base standard, UL 2900-1, describes documentation and risk management and risk control requirements that are useful not only for the stated purposes, but also for setting design requirements. The standard also describes testing and evaluation methods. The specific standard, UL 2900-2-1 tailors the base standard requirements for application to medical devices. Both standards will prove useful to the intended audience of this report. UL has produced a webinar on the 2900 series standards to provide additional assistance with their use [49].

Because of their usefulness, and because Health Canada references them in its guidance document [13], they are recommended reads. Both can be purchased from the UL webstore or via the Standards Council of Canada (SCC).

5.1.2 AAMI TIR57

AAMI TIR57 “Principles for medical device security – Risk management” [21] nominally addresses cybersecurity risk management for medical devices. To do so, the report considers: threat, vulnerability and asset identification; estimating, evaluating and

controlling risk; and, monitoring the effectiveness of risk controls. Additionally, beyond these subjects, the report also describes: generating cybersecurity requirements; identifying security characteristics; and, applying the methods and techniques described in the report to a theoretical example. Thus, TIR57 is a feature rich document. Health Canada also references TIR57 in its pre-market guidance document. It can be purchased from the AAMI webstore.

Sections 7.1, 7.2 and 9 consider TIR57 further.

5.1.3 Common Criteria

As stated earlier in section 1.1.2, the Common Criteria (CC) is an international program in which Information Technology (IT) products are certified against standard specifications called Protection Profiles (PPs). There are over 200 Protection Profiles (active and archived) covering a variety of devices and systems including biometric devices, smart cards, key management systems (see section 4.2), computer operating systems and even cell phones. However, there are no PPs that specifically cover medical devices. Initially, the NRC and the CSE had considered developing PPs for certain types of medical devices including implants, remote patient management systems, and mobile apps. After some deliberations this approach was not pursued because of the following reasons:

1. The CC program is used to certify IT products and systems for use in government IT systems. Because of the highly sensitive nature of some government related IT systems, use of CC may be overkill for most medical devices.
2. Because of 1, certifying a device to a PP is expensive, possibly prohibitively so, for most medical device developers (see section 7.3.2).
3. Existing PPs cover enough different variations of IT equipment that appropriate ones may be found and leveraged for use with most implementations of medical devices.

The use of existing PPs is explored further in sections 7.1, 7.3.2 and 9.4.1. In particular, four will be leveraged. These are:

1. “Protection Profile for Application Software” [50]
2. “Protection Profile for Mobile Device Management” [51]
3. “Protection Profile for Mobile Device Fundamentals”, [52]
4. “collaborative Protection Profile for Network Devices” [53].

5.1.4 IEC 80001 Series

IEC 80001 is a set of standards and technical reports with a base title of “Application of risk management for IT-networks incorporating medical devices” [54]. There are 11 documents in the set. They consider the incorporation of connected medical devices into a clinical IT network such as that found in a hospital. Because of this, they are more applicable to a user of a connected medical device than to a developer.

5.2 Reports

5.2.1 UL IoT Top 20

In addition to the 2900 series standards, UL has produced a document entitled “IoT Security Top 20 Requirements” [20]. While specifically targeted for the protection of IoT, most of these 20 requirements are applicable to medical device cybersecurity with the exception of 11 (which allows for users to enable on-demand features they may use intermittently). Section 7.1 considers these requirements further.

5.2.2 UK Government Secure by Design

The UK government ministry responsible for digital technology has produced a report “Secure by Design: Improving the cyber security of consumer Internet of Things” [55] which includes a Code of Practice [56]. While targeting consumer IoT products, there is sufficient overlap with medical devices that the Code of Practice (CoP) can be used by medical device developers, and in fact, is utilized later in this report (see sections 7.1 and 9). Note that CoP item 10 pertains to users rather than device developers and so can be ignored by device developers.

5.2.3 PETRAS Summary

The PETRAS IoT Research Hub is a consortium of nine UK universities working together to research issues in privacy, ethics, trust, reliability, acceptability and security (PETRAS). They have produced a report “Summary literature review of industry recommendations and international developments on IoT security” [57], which includes an overview of principles and practices for IoT security, which can be applied to connected medical devices. This is utilized later in this report (see sections 7.1 and 9).

5.2.4 British Standards Institute White Paper

The British Standards Institute has a white paper report “Cybersecurity of Medical Devices: Addressing patient safety and the security of patient health information” [58] which includes a discussion of the dichotomy between risk analysis for medical device safety versus medical device cybersecurity. This is explored further in section 7.2.

5.2.5 Medical Device and Health IT Joint Security Plan

The Joint Security Plan (JSP) was prepared by the Healthcare and Public Health Sector Coordinating Council (HSCC), which is a US public-private partnership between private-sector critical healthcare infrastructure entities (such as hospitals, clinics, health insurers, medical device companies, cybersecurity companies (such as Mitre) and industry associations (such as AAMI)) and the US government. The HSCC describes the document as a ‘consensus-based total product lifecycle reference guide for developing, deploying, and supporting cyber secure technology solutions in the health care environment” [59, p. 8]. The JSP describes a security framework, similar to the NIST Cybersecurity Framework (see section 4.7) but with a focus on products. As such, it is a very comprehensive document. The main body of the document discusses:

1. Risk management, including product security risk assessment
2. Design controls, including requirement identification and security testing
3. Post deployment considerations, including decommissioning

4. Evaluation of organizational cybersecurity maturity

The JSP has eleven appendices. Appendix D contains a link-enabled list of all the references used to develop the plan. Appendix E contains a list of 37 example security requirements. Appendix G suggests the types of information to be included in the documentation package for a device. It includes a brief discussion of a software Bill of Materials (BoM) (see section 8.1).

5.3 Related Resources

5.3.1 NIST Reference Designs

As mentioned in 3.1, the NIST NCCoE is preparing a cyber-secure TeleHealth Remote Patient Monitoring (RPM) reference design which will be freely available upon completion [23]. The NCCoE website[7] should be examined periodically in order to keep abreast of its development. Additionally, the NCCoE also has two completed reference designs: the first is “Securing Electronic Health Records on Mobile Devices” [60]; the second is “Securing Wireless Infusion Pumps in Healthcare Delivery Organizations” [61]. The first reference design is, like AAMI TIR57, quite feature rich. In particular, the risk analysis is very detailed, both in terms of methodology and actual results [60, p. 194]. This risk analysis should prove particularly useful as a starting point for a medical device developer with interests in using mobile devices as a medical device. Additionally the first reference design contains a detailed description of the testing needed [60, p. 209]. The wireless infusion pump reference design, while also detailed, is more applicable to the creation of a cyber-secure hospital network of medical devices, rather than to a cyber-secure medical device. Both are available free of charge from the NCCoE website.

5.3.2 OWASP

The Open Web Application Security Project (OWASP) is a not-for-profit organization focused on improving the security of software, specifically web based applications [62]. It has a variety of flagship projects focused on three areas: tools; code; and documentation. OWASP provides the following at no charge and with no restrictions:

- Application security tools and standards
- Documentation on security testing, as well as secure code development and review
- Concise collections (``cheat sheets``) of high value information on specific application topics

The OWASP document on testing [63] is quite comprehensive, providing detailed testing instructions along with a higher level description of other techniques that OWASP considers part of testing, including deriving security requirements, threat modeling and source code reviews. It also describes a testing framework which commences even before development begins. This framework is similar in nature to the NIST Cybersecurity Framework (see section 4.7) and offers an alternative framework implementation.

[7] https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth

5.3.3 CSA Cyber Verification Program

The Canadian Standards Association (CSA) is currently developing a standard to address cybersecurity aspects of a product and the organization developing that product. It has been proposed as a National Standard of Canada [64]. The Cyber Verification Program (CVP) consists of a self-assessment, onsite audit and formal product testing and evaluation. This program is built on the premise that an insecure organization cannot build a secure product. Security practices must be embedded into the organization's operations and development processes. The assessment considers six domains and eighteen practice areas within these domains. The current self-assessment consists of 198 binary questions that, once completed in connection with an audit, will provide a maturity rating for the organization.

The program has been field tested and has resulted in a Notice of Intent (NOI) being filed that will lead to a standard being developed for the Canadian marketplace. This will include the ability for vendor organizations to perform an attestation to this standard. While the CVP is in its infancy, medical device developers should be aware of it and monitor future developments.

Recommendation

Read UL2900 series, TIR57 and relevant Protection Profile first

6 Health Canada Pre-market Guidance Document

The Health Canada draft Pre-market guidance document [13] is considered in this section. The guidance document consists of two primary sections: an Introduction and a Guidance for Implementation. Salient points within both sections are repeated.

6.1 Policy Statements (section 1.2)

This section of the guidance document calls for a medical device developer to consider a number of issues, including:

- Designing cybersecurity into the device from the start; therefore, cybersecurity related design requirements should be developed and documented in concert with those requirements that address the functional, performance and safety aspect of the device.
- Incorporating cybersecurity concerns into their risk management process.
- Developing and maintaining a cybersecurity framework (see section 4.7 of this report).
- Verifying and validating device cybersecurity performance against design requirements.

6.2 Guidance for Implementation (section 2)

This section of the guidance calls for a medical device developer to have a strategy to address cybersecurity risks to their device. This strategy is to include the following elements:

- Secure design: A developer must consider cybersecurity risks and controls when making design choices; design choices should maximize cybersecurity while not unduly hampering safety critical aspects of the device (see section 8.2 of this report). Some suggested cybersecurity related design principles are shown in Table 1 of the guidance document. These are discussed further in sections 7.1 and 9.2.1 of this report.
- Risk management: An experienced medical device developer should already be familiar with the safety related risk management process as described in ISO 14971 [18]. A similar process is needed to manage cybersecurity related risks. However, there are some differences between the two processes, which are discussed further in section 7.2 of this report. Because of the differences, a cybersecurity risk management process should be conducted in parallel with the safety risk management process. These parallel processes are shown in figure 2 of the guidance document [13]. The two processes cannot be conducted in isolation, as a cybersecurity risk control may adversely impact safety, and vice-versa. These impacts must be considered anytime a resulting new risk is mitigated.
- Verification and validation testing: As is the case with any medical device development, testing must be performed to show that the device's behavior and performance matches its design requirements. The cybersecurity related verification and validation testing is discussed further in section 7.3.
- Post deployment monitoring and response: After a medical device is fielded, the developer will have to address reports of adverse behavior from users; additionally the developer will need to keep track of new vulnerabilities that may affect their device as these vulnerabilities are discovered and recorded. Other expected actions may include continuous post-market vigilance, patching, third party vulnerability disclosure mechanisms, and information sharing. Section 7.4 of this report discusses these actions further.

Each one of these elements is discussed in more depth in the following section.

7 Implementation of the Strategy

Each element in the strategy to address cybersecurity risks called for in the Health Canada Pre-Market Guidance is discussed here.

7.1 Security by Design

Annex C of TIR57 [21] addresses generating cybersecurity requirements. The first statement in this Annex is quite illuminating, "The backbone to security risk management is the ability to express the medical device security behaviours … in the form of verifiable requirements" [21, p. 37].

To help the developer in creating this backbone of verifiable requirements, the various documents described in section 5 (particularly the UL List of IoT Security Top 20 Requirements [20], the four Common Criteria PPs [50] [51] [52] [53], the UK Secure by Design Code of Practice [56] and the PETRAS Summary [57]) can be used as a checklist of items to consider, as can Table 1 of the Health Canada Pre-market Guidance document [13]. Table 9 in Appendix A cross-references the Health Canada suggested design principles with the requirements from these other references. Notice that many of the same requirements (perhaps stated somewhat differently) appear in the various lists. Also note that this list is far from exhaustive, and that several of the CoP, UL, PETRAS and PP requirements are not present in the table in Appendix A, but still should be considered by the developer.

One of these requirements is UL Top 20 number one “Provide a manual override for any safety critical operations.” This requirement is explored further in section 8.2.

Besides the UL Top 20, UK CoP, PETRAS and PPs mentioned above, a review of UL 2900 [47] [48] and TIR57 [21] at some point during requirement formulation may prove beneficial. Annex D of TIR57 “Questions that can be used to identify medical device security characteristics” [21], is particularly helpful in this regard. For those developers familiar with ISO 14971 [18], TIR57 Annex D is similar to Annex C of 14971 “Questions that can be used to identify medical device characteristics that could impact on safety”; both are “*aide-memoire*” to remind the developer of items to consider. Appendix E of JSP also contains suggested security requirements [59].

As the developer finalizes the cybersecurity requirements for their device, and incorporates these requirements into their overall design process, particular implementation options (allocation of functions to software versus hardware, identification of specific hardware components (computers, integrated circuits etc.) and of specific software stacks (OSs, frameworks, libraries, languages etc.)) will be explored. As part of this exploration, the developer should consider the impact of the usage of the identified components and stacks, by, for example, querying the CVE (see section 4.5) but perhaps more importantly, by incorporating their impact into the developer’s cybersecurity risk management process.

Recommendations

Generate a list of security requirements using the resources described above

Query the vulnerability databases when choosing between design options

Ensure that a secure post deployment software update mechanism, such as using code signing, is designed into the device

7.2 Cybersecurity Design and Risk Management

As mentioned in section 6.2, a medical device developer must manage cybersecurity risks just as they must manage safety-related risks. The two processes are very similar in that each involve risk estimation/analysis, evaluation and control steps. However, the two are divergent in the following ways:

1. The determination of the probability of a cybersecurity event (analogous to a harm in the safety sense) is difficult in the absence of data or even the knowledge that an event is possible [58, p. 9], whereas a similar determination of the probability of a safety harm can rely on a large body of established information [18, p. 10].
2. The safety definition of harm ("physical injury or damage to the health of people or damage to the property or environment" [18, p. 1]) may result in a cybersecurity risk not being addressed, if the effect of a cybersecurity attack results in no physical injury or damage.

Because of this divergence, Health Canada and AAMI recommend that a separate cybersecurity risk management process be undertaken in parallel with a medical device developer's traditional safety risk management process [13] [21]. As also described in section 6.2, the two processes cannot be conducted in isolation, as a cybersecurity risk control may adversely impact safety, and vice-versa. For example, adding an authentication regime to a device may render it inaccessible in the event of an emergency if a user cannot remember a password while under emotional stress. Similarly, adding a network connection to a device without proper cyber controls may have no impact on patient physical safety, but may act as an easily exploited cyberattack access point. Figure 2 in the Health Canada Pre-market Guidance document [13] illustrates this consideration further. Note that as a risk is mitigated in one process, the effect of the mitigation on the other process must also be considered.

The steps in the security risk management process are:

1. Risk management plan preparation
2. Risk analysis
3. Risk evaluation
4. Risk control implementation
5. Residual risk evaluation
6. Report preparation
7. Post deployment surveillance and response

The risk analysis portion of the process should consider each of the following elements: [21, p. 9]

1. Intended use;
2. Security characteristics of the device, such as authentication methods and implemented communications protocols[8];
3. The operating environment for the device including device parameters expected to be configured by the user;
4. Threats;
5. Vulnerabilities;
6. Assets along with adverse impacts to these assets, should an attack occur;
7. An estimate the risk for each threat and vulnerability combination.

[8] See Annex D of TIR57 for questions to help identify device security characteristics

The combination of threat and vulnerability is analogous to the probability of occurrence in the safety risk process, while the impact on the asset is analogous to the severity of the harm [21, p. 11]. The risk then is the combination of these three factors [21, p. 25]. With this information, the developer can determine if the risk is acceptable, or needs to be mitigated by some control. If mitigation is required, a determination of the residual risk is required, following the same risk analysis process.

TIR57 recommends that an existing security risk analysis for a similar medical device be used as a starting point for any new risk analysis [21, p. 9]. As will be described in section 9.3.1, the TIR57 theoretical system, the Kidneato artificial kidney, comprises all aspects of a connected medical device. Therefore, the risk analysis performed for it can be used as a starting point, in the absence of any alternatives. Note that an alternative starting point for applications involving mobile devices is the risk analysis performed for the NIST reference design “Securing Electronic Health Records on Mobile Devices” (see section 5.3.1).

As the design matures and becomes ready for manufacture and deployment, both the safety and cybersecurity risk processes must be updated. As part of this, test results will be needed.

Recommendations

Use an existing security risk analysis as a starting point.

Consider the effect of the cybersecurity risk process on the safety risk process, and vice versa.

Consider the threats enumerated in the Protection Profiles referenced above.

7.3 Testing

Besides the testing needed to show safety and effectiveness, a medical device developer will have to perform cybersecurity related testing to show that their device meets its cybersecurity requirements. The tests recommended by the Health Canada Pre-market Guidance document [13] are those described in UL 2900-1 and 2900-2-1. Note that a developer enjoys sufficient latitude to employ other tests, provided that these accomplish the desired goal of showing that the device meets its cybersecurity requirements. Additionally, the tests called for by UL 2900-x are test categories rather than specific tests, so specific tests from other authorities could be used if they fall into one of the UL 2900 categories.

7.3.1 UL 2900-1 and UL 2900-2-1

These standards call for the following tests:

1. Known vulnerability testing – this is not testing per se; instead the NVD should be consulted to determine if any of the device’s components (hardware and software) have known vulnerabilities (see 4.5).
2. Malware testing – the device’s software is scanned by the malware tools applicable to the operating system on which it is to be installed.

3. Malformed input testing – here, the device is presented with invalid or unexpected inputs on its external interfaces. The device should continue to operate as expected in all cases.
4. Structured penetration testing – here the device undergoes a simulated cyberattack. There are two different types of penetration testing: black box, and white box. In a black box test, the test conductor has no knowledge of the device, while in a white box test, the test conductor is familiar with the design of the device. Assuming the device developer is at least assisting with penetration testing, then white box testing is being performed.
5. Software weakness analysis – like item 1, this is not testing per se but an analysis performed using the CWE.

Some tools used to perform various aspects of cybersecurity testing are shown in Table 3.

Test type	Examples of Tool	Comment
Vulnerability scan	Nessus [65] OpenVAS [66] Nmap (XSE scripts) [67] Nexpose [68]	Assists in vulnerability assessment activity. Tends to have many false positives that require analysis.
Port scan	Nmap (Zenmap is the Windows GUI version)	Often covered as part of the vulnerability scan, but helpful to compare results.
Packet analysis and capture	Wireshark [69] TCPDump [70]	Useful for determining what the device is actually doing when talking to 3rd parties
Packet manipulation and crafting	Metasploit [71] Scapy [72]	Allows for creation of malformed packets and special payloads to provoke responses from the product. Requires a great deal of expertise to be effective.
Cookie manipulation	Firebug [73] (Browser Extension for Firefox)	
Man in the middle (MiTM) (proxy)	Ettercap [74]	Not very user friendly and prone to breaking, but the most common/popular tool for doing MiTM using ARP[2] poisoning
Automated malformed input[1]	Peach Fuzzer [75] TAOF [76]	
Note 1: Also known as “Fuzzing”; performed by inputting massive amounts of random data (the fuzz). SQL injection is a specific type of malformed input testing. Note 2: ARP is Address Resolution Protocol		

Table 3: Cybersecurity Testing Tools

7.3.2 Common Criteria

The majority of Protection Profiles (PPs) within the Common Criteria (CC) scheme specify very detailed tests to be performed for each of the associated functions. This is one of the potential benefits of leveraging a PP: once a developer has finalized their design requirements for the device, the requirements can be mapped to PP Security Functional Requirements (see Table 9 in Appendix A) which have associated tests with very specific

pass/fail criteria. This greatly simplifies test planning and analysis. It also offers the additional benefit of leveraging the testing infrastructure associated with the CC. In Table 3 of Health Canada's Pre-Market Guidance document [13], the use of cybersecurity experts familiar with structured penetration testing is recommended. As part of CC, the CSE accredits IT security testing labs. This is analogous to safety testing labs such as QPS, Entela and CSA being accredited to perform medical device electrical safety tests. Security testing can be expensive; testing costs can range from tens to hundreds of thousands of dollars [77]. Part of this expense is the determination of what tests need to be performed and how to evaluate their outcome. This expense can be decreased with the approach described above [46].

7.3.3 OWASP Testing Guide

As described in section 5.3.2, the OWASP Testing Guide [63] is quite comprehensive, providing detailed testing instructions for applications developed for the web. For such applications, the Testing Guide can be used for the same purposes described for PPs in section 7.3.2.

Recommendations

Use the Protection Profiles listed above and the OWASP Testing Guide to help define necessary tests.

7.4 Post Deployment

After a connected medical device has been fielded, the device developer will need to employ the CVE and related cybersecurity infrastructure (see section 4.5) to keep track of newly reported vulnerabilities that could impact the fielded device. This activity will need to be done on a regular basis. Additionally through the surveillance process established as part of ISO 13485, the developer should receive complaints from users of the fielded device should a cybersecurity related issue be discovered by them. These complaints will need to be investigated. If a vulnerability is discovered as a result of the investigation, and this vulnerability could lead to patient harm, then it may need to be reported to Health Canada. The risk assessment for the fielded device will have to be revisited in light of this new vulnerability and the potential for patient harm reassessed. In any event, the new vulnerability should be reported to an ISAO (see section 4.6). In most cases, a patch that addresses the exposed vulnerability will need to be deployed. This deployment will utilize the mechanism for secure software updates that satisfies the initial design requirement (see section 7.1) and that was validated during testing (see section 7.3). This same cyber robust software update process will be employed whenever a non-cybersecurity related patch or software update is pushed to the fielded device.

Recommendation

Consider joining an ISAC/ISAO

Check the vulnerability databases regularly for new vulnerabilities

Revisit the cybersecurity risk analysis as new vulnerabilities arise

Update the software regularly using a secure update mechanism

8 Other Important Topics

There are several topics not previously discussed in this report for which a medical device designer needs to be aware.

8.1 Software Bill of Materials

The Health Canada Pre-Market Guidance document [13] requires a software Bill of Material (BoM) as part of the labelling for the medical device (Note that the US FDA refers to this as a Cyber BoM or CBoM). This BoM should list all custom developed code along with third-party or open source software used in the software build. The rationale for this is the BoM allows the device user and other interested parties to make a determination if a device is at risk as vulnerabilities are found, or as cybersecurity events occur. While seemingly straightforward, the following concerns associated with a software BoM have been raised [78]:

1. Publically exposes proprietary code
2. Promotes cyberattacks if the software BoM is obtained by a threat actor
3. Overstates a risk if a component is present in the BoM, but is not in fact exploitable
4. Becomes unwieldly if libraries within libraries are included

The benefits of having a software BoM in the hands of users probably exceed the risks of a threat actor exploiting the information. As risk management is a central concept in medical device development, users need to be able to make informed decisions related to cybersecurity. The software BoM increases a user's ability to make an informed decision. Additionally, in the opinion of cybersecurity researchers, threat actors are capable of quickly determining the information to be found in any given software BoM anyways should they wish to do so; therefore it is imperative that legitimate users be provided this information [79].

Also note that maintaining and documenting software versions is required by IEC 62304, which is on the list of standards recognized by Health Canada, and so this information should be readily available for incorporation into a BoM. As to implementation, a software BoM appears similar to a Version Description Document [80] that was used extensively at one time for software developed for government agencies; templates exist that can help to prepare a software BoM. Deliberations regarding the best way to implement a software BoM are ongoing [79].

Recommendation

Prepare and maintain a software bill of material

8.2 "Break Glass" Emergency Override

As mentioned in section 7.1, the first of UL's Top 20 IoT Requirements [20] is to "provide a manual override for any safety critical operations". This override concept is sometimes referred to as "Break Glass in Case of Emergency", or simply "Break Glass"; in the event of an emergency, should a cybersecurity control prevent a user from conducting a safety

critical operation, the cybersecurity control should be overridden. While this appears to be a simple concept, the implementation may prove very complex. As a device is made more impregnable, it risks inadvertently locking out a legitimate user at a very inopportune time (see section 7.2).

Some suggested design implementations are:

1. Override should be truly manual, involving a physical control (such as a switch) on a device; this eliminates any SaMD (Software as a Medical Device), and any override commands being made over a network connection.
2. All network connections should be disabled, so that no threat actors can use the override as an access method. Furthermore, re-enabling of the connections should not be accomplished by a simple power off reset.
3. Immediately before the network connections are disabled, an unalterable message should be sent to the associated network administrator as to the triggering of the Break Glass override. This should initiate a recovery process that will necessitate physical access of the device by designated network personnel.

TIR57 also considers emergency access [21, p. 19] [21, p. 47].

Recommendation

Determine if an emergency override is required.

8.3 Labelling and Related Documentation

The following cybersecurity related information needs to be incorporated into the labelling and related documentation for the device [13, p. 12]:

1. Software bill of material (see section 8.1);
2. Any particular hardware or software requirements for a host computer or mobile device, if this equipment is not supplied as part of the device;
3. Instructions (if needed) for a patient or user to properly configure the device;
4. Instructions (if needed) for IT personnel to properly accommodate the device on their network;
5. Information on acceptable residual risks present in the device and for which the user, patient or IT personnel needs to be notified [21, p. 12];
6. Instructions for the user, patient or IT personnel to respond to, recover from, and report a cybersecurity event;
7. Instructions (if needed) for the user, patient or IT personnel to update the device software, or information on what to expect should the device update its software autonomously, and what steps should be taken should an autonomous update fail;
8. Instructions to return the device to service should an emergency override be invoked (see section 8.2).

This information needs to be present in any package inserts, device product brochures, file cards, and any webpages specific to the device.

Additionally, the FDA has recommendations for cybersecurity related labelling in its latest Premarket Guidance document [44, p. 18]. A developer may also want to consider including some of these recommendations in its labelling.

Recommendation

Ensure that cybersecurity related information is incorporated into the device labelling.

8.4 Licence Applications

A medical device licence or licence amendment application needs to contain the following cybersecurity related information [13, p. 12]:

1. Risk management report prepared at the conclusion of the risk management process described in section 7.2;
2. Summary of reported problems and details of any cybersecurity related recalls;
3. For class IV devices, a quality plan that demonstrates the incorporation of a cybersecurity framework;
4. List of cybersecurity related standards applied during the design and manufacture of the device;
5. For class III devices, a detailed summary of the cybersecurity testing results;
6. For class IV devices, all cybersecurity testing results;
7. A traceability matrix that maps identified cybersecurity risks to:
    a. Requirements specification (design inputs),
    b. Design specifications (design outputs), and
    c. Verification and validation tests.
8. A summary of the maintenance plan for the device describing the software update mechanism and the post-deployment process to be followed to ensure the device's continuing cybersecurity.

Recommendation

Ensure that all necessary cybersecurity related information is incorporated into the licence application.

9 Illustrative Example – bConnected

As mentioned in 3.1, bConnected is a research platform for the purposes of interactive remote patient monitoring and management being developed by the Simulation and Digital Health (S&DH) section of the Medical Devices Research Centre (it was still under development when this document was prepared). It is descended from the section's successes in developing telesimulation devices used to deliver health care training remotely [81]. It has some commonality with Remote Patient Monitoring (RPM) medical devices and so is examined from this perspective. Considering an RPM-like system like bConnected is beneficial because such a system, like the Kidneato example in TIR57, encompasses parts of a medical device (interactions with patients, with primary

caregivers, with clinicians and with other aspects of a clinic and a hospital). The Kidneato system includes an implanted device that mimics the functioning of a kidney; that is, it delivers therapy automatically. As such, any cybersecurity event that negatively impacts this therapy could result in severe harm. bConnected's research motivation is to allow a clinician to remotely monitor various patient physiological parameters. It delivers no therapy, the connected devices used to measure the parameters are non-invasive, and a clinician analyzes and interprets the measurements. The more benign nature of bConnected is shown in possible use statements suggested for the system.

9.1 bConnected Intended Use / Indications for Use

Intended Use and Indication for Use statements for bConnected follow.

9.1.1 bConnected Intended Use

bConnected is an interactive remote monitoring research system intended for use by healthcare professionals for continuous collection of photoplethysmograms (PPG) and galvanic skin resistance (GSR) data from patients in home and healthcare settings. Data is transmitted wirelessly from connected sensors to the bConnected mobile component from which it is further transmitted to a central server for storage, retrieval and analysis. The bConnected central server application can include the ability to notify healthcare professionals when physiological data fall outside selected parameters.

The data from the bConnected system is intended for use by healthcare professionals as an aid in diagnosis and treatment. It is not intended for use on critical care patients nor to replace standard monitoring and/or routine care.

9.1.2 bConnected Indications for Use

bConnected is indicated for use on adult patients 18 years of age or older with cardiovascular diseases and in situations when the clinician believes closer monitoring of PPG and GSR parameters associated with these diseases is warranted.

9.2 bConnected Security by Design

9.2.1 Top Level Functional Requirements

The basic functional requirements for bConnected are:

1. Acquire patient data (clinical and administrative) from PPG and GSR sensors.
    a. Data to be acquired either manually or electronically.
2. Transfer acquired patient data to a repository for storage and access.
3. Allow patient data to be examined, shared, visualized, analyzed and aggregated.
4. Support S&DH research and development efforts such as those related to assessment and remediation of cognitive deficits.

9.2.2 Security Functional Requirements

Using the method described in section 7.1, the following security functional requirements are proposed. Some are written to illustrate potential pitfalls that are best avoided in

requirements statements (see Annex C of TIR57 [21, p. 37] for further information on this subject).

1. All exchanged information (whether transmitted by wire or wirelessly) must be sent securely, using industry standard security protocols.[9]
2. All credentials and personally identifiable information must be stored securely.
3. Mutual authentication is required for information exchanges between the various components of the system.
4. A proper access control management mechanism is required. The requirement for access control could be stated two ways:
    a. All users must be authenticated and authorized. Access control methods using the principle of least privilege should be implemented. This principle is a universally accepted cybersecurity best practice for system access control; or,
    b. The system should clearly define different categories of user, each with specific types of access rights.
5. Software updates will use a trusted update mechanism.
6. No emergency overrides will be permitted, as none of bConnected's functions are safety critical.
7. Access logs will be created and maintained. For bConnected, detailed action logs are created and maintained to track all activities within the system.

These requirements (with the omissions noted) along with the basic functional requirements can now be used by developers to make design choices. As such choices are made (for example the different user categories mentioned in 4), they should be considered in the risk analysis, documented in a design specification and considered during test planning. This process allows for the creation of the traceability matrix required as part of a licence application (see section 8.4).

9.2.3 Initial Design Concept

With the functional requirements as given in sections 9.2.1 and 9.2.2, an initial design concept was developed (see Figure 1) with the following details:

1. bConnected utilizes a GraphQL API architecture, providing functionality as a number of Web services.
2. The various components of bConnected (mobile application, front end, back end, security services (authentication, authorization, access control)) communicate via HTTPS methods, with the payload information formatted as JSON strings. Note that the decision to use HTTPS (vice HTTP) will improve the cybersecurity of

[9] A possible concern is what constitutes "industry standard". The clause after "sent securely" should be omitted.

bConnected (assuming proper implementation; testing will have to prove this) and will satisfy the first security functional requirement. It also will require that the various components of bConnected be properly configured with the appropriate certificates (see section 4.2) upon deployment. Should a license application for bConnected be made, then deployment related considerations need to be included in any labelling developed for bConnected.

3. bConnected uses a token based authentication approach, i.e. the JSON Web Token (JWT). JWT is an open standard for securely transmitting information between parties as a JSON object [82].
4. bConnected stores critical user data in its backend server. But it also supports a temporary storage solution for sensor and device readings, together with non-identifiable information such as patient ID, in clear text on the mobile device if communication with the backend is not available when the measurements are acquired. Upon re-establishment of a successful network connection, transmission will be automatically resumed, and the temporary local storage file will be deleted.
5. With respect to user access, bConnected supports the following implementation:
    a. All users must be authenticated and authorized. Access control methods using the principle of least privilege will be implemented.
    b. The system supports three categories of user, with different levels of access to information:
        i. Patient and caregiver – can access patient data only; access is restricted to viewing existing data and adding new readings.
        ii. Clinician (doctor and nurse) – can access patient data for all patients managed by the particular clinician; access is restricted to viewing existing data and adding new readings (to allow for readings to be entered while patient visits clinician); can modify administrative data identifying clinician.
        iii. Administrator – can access and modify all patient and clinician data.

The rationale behind 5.b is that bConnected is designed not only to be a patient management focused system, but also to include a social life style modification approach. To support such a concept, fine-grained access control is implemented to support both peer information sharing among patients and caregivers, and also potential collaboration among clinicians.

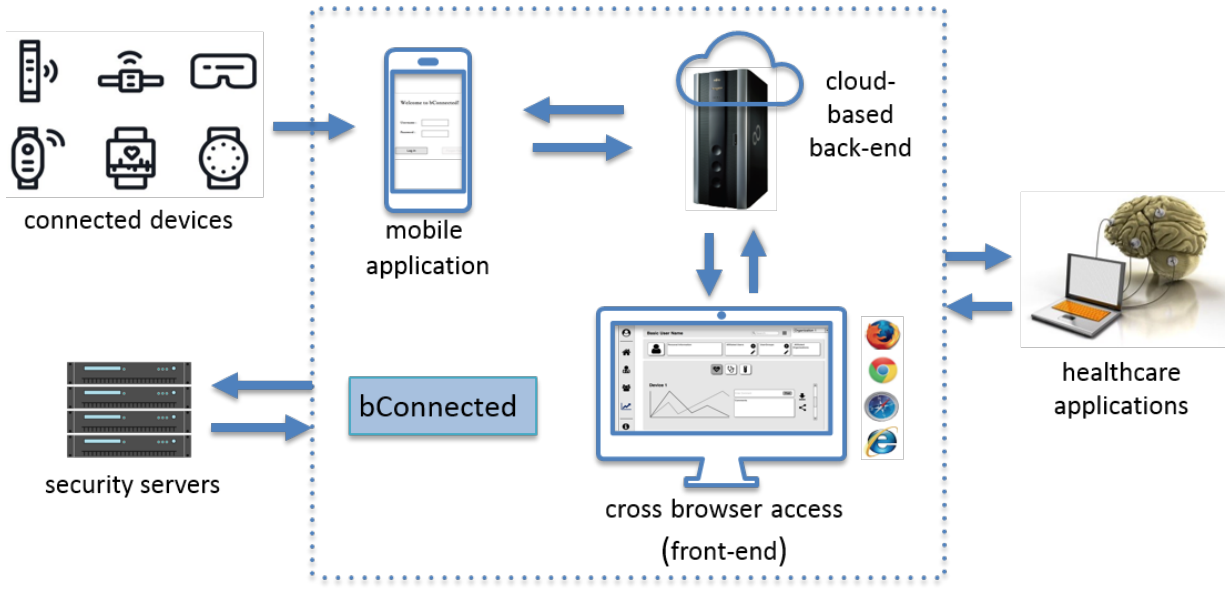

Figure 1: bConnected Initial Design Concept

9.2.4 Initial Design Choices

With the design concept described in 9.2.3, the following implementation choices were made:

1. Django framework for back-end;
2. React for front-end;
3. MongoDB database on back-end;
4. GraphQL (Graphene) as API architecture;
5. JWT for authentication and authorization; and
6. React Native for mobile application development.

As a common practice, most application developers maintain a list of libraries and other required software components in a configuration file. The main purpose of such a file is to allow for automated configuration of a developer's environment and to prepare for the final deployment process. It can also be used to create the software bill of material needed as part of the device's labelling (see sections 8.1 and 8.3). Additionally, the configuration file can be used to guide the search of the vulnerability databases described in section 4.5. Such a search should be conducted in concert with the initial design choices and then repeated as additional libraries are added.

As an illustration of this purpose, Table 4 shows the contents of the configuration file used for the bConnected back-end (at the time of writing of this document), along with the number of vulnerabilities reported for each library. The number after the library component name corresponds to a particular required version.

Library component	CVE	NVD
mongoengine==0.15.0	0	0
Django	85[1]	86[1]
graphene_django==2.0.0	0	0
django-cors-headers	0	0
django-graphql-jwt==0.1.10	0	0
Pipreqs	0	0
graphene-mongo	0	0
1: NVD number falls to 2 when Django 2.0.1 is specified (as opposed to Django alone). CVE number increases to over 450.		

Table 4: Back End Requirements File With Vulnerabilities

As can be seen in Table 4, there are no reported vulnerabilities for all of the libraries except for Django. Entering “Django” without a version number results in 85 and 86 reported vulnerabilities for the CVE and NVD respectively. Entering “Django 2.0.1” results in 2 for NVD and 453 for CVE. (NVD “ands” the two terms, while CVE “ors” them. A developer should note this discrepancy in search methods between the two databases).

To address these two vulnerabilities, the Django Software Foundation issued security releases with the resulting version of Django becoming 2.0.11. This release needs to be incorporated into bConnected at some point during its development (which was still ongoing when this document was prepared), with the latest possible time being immediately before formal verification and validation testing is undertaken. In general, incorporating patches to library components as they arise is good practice, as this should minimize any potential disruptions (particularly schedule slips) that could occur as a result of the change.

A similar process can be undertaken for the remaining components of bConnected; that is, for the front-end and the mobile component.

9.3 bConnected Security Risk Management

Once the initial design choices are made, the risk analysis portion of the security risk management process (see section 7.2) can commence.[10] As described in section 7.2, TIR57 recommends that an existing security risk analysis for a ***similar medical device*** be used as a starting point. In the absence of an existing analysis, the fictional Kidneato example in Annex E of TIR57 can be used as it “can also represent a wide range of medical devices and accessories” and “rather than the specific medical function”, it is “the

[10] The preparation of the risk management plan can start prior to any design activities however.

location, communication, processing, data storage (that) are of the primary importance" in a cybersecurity risk analysis [21, p. 49]. This is explored further in the next section.

9.3.1 TIR57 Kidneato Description and bConnected Comparison

The Kidneato system comprises the following elements:

1. An implanted artificial kidney: Besides acting as a kidney, it communicates wirelessly with a programmer used in a clinic or hospital setting, and a wireless communication accessory used in the home. It represents any medical device that is implanted in or located external to the body, and which interacts with the body in some medically useful way. An MRI unit or a heart rate sensor (such as used in bConnected) are alternatives for this element.
2. Hospital based programmer: It communicates wirelessly with the implant for initial setup of the implant following surgery and then for monitoring and parameter modification during subsequent patient checkups. It represents any medical device or accessory which connects to a managed network such as that found in a hospital and which has wireless and wired connections and other interfaces such as USB. An infusion pump or vital signs monitor are alternatives for this element. There is no equivalent in bConnected.
3. Home based wireless communications accessory: This interacts wirelessly with the implant for charging and data communication. It also communicates wirelessly with a mobile app on a patient supplied mobile device. The mobile app in turn also communicates over a public network. Together these three items represent any medical device or accessory used in an uncontrolled environment connected to a public network such as the home. The GSR and PPG sensors, along with the mobile device and bConnected mobile app are alternatives for this element.
4. Users: This element includes patient, family, caregiver, clinicians and network administrators which interact with the preceding three elements using dedicated applications or web browsers installed on a variety of different computing platforms. The same users are expected for bConnected (and indeed for all connected medical devices), with the bConnected front end an alternative for the Kidneato's dedicated applications or web browsers.
5. Web services: This element consists of multiple servers, possibly cloud based, and provides web services such as authentication and patient databases. The bConnected back end is an alternative for the Kidneato's web services element.

As there are bConnected alternatives for the various Kidneato elements, the risk analysis for the Kidneato system can be used as a default starting point for bConnected. A similar analysis can be used to validate use of the Kidneato risk analysis as a default starting point for other medical devices, should other more appropriate analyses be unavailable.

Block diagrams showing the various Kidneato elements can be found in Appendix B.

9.3.2 TIR57 Analysis Methods

As described in section 7.2, cybersecurity risk is a combination of threats, vulnerabilities and impact on assets. TIR57 describes three approaches [21, pp. 34-35] which are best

illustrated by examples from the Kidneato analysis, which follow. The tabulated approach and assessment values are in accordance with NIST SP 800-30 [83].

9.3.2.1 Starting With Vulnerabilities

Vulnerability	Likelihood of exploit	Impact	Risk	Mitigating Control	Residual Risk
No password policy for Web services - “password” is acceptable	Very high – password guessing is common attack	High – attacker gains access easily	Very high – particularly if user privilege assignment is also very lax	Policy requiring complex passwords that change periodically	Acceptable
Maintenance password is hard coded	High – documentation contains password	Very High – attacker gains elevated privileges	Very high	No hard coded passwords	Acceptable
Connections with APIs are potential attack vectors	Low	Low	Acceptable	None	Acceptable

9.3.2.2 Starting with Threats

Threat	Vulnerability	Likelihood	Impact	Risk	Mitigating Control	Residual Risk
Attacker reads patient data	Data sent unencrypted	Medium	Medium – patient data exposed	Medium	Encrypt all transmitted data	Acceptable
Attacker changes device firmware	Software updates not authenticated	Low – requires sophistication	Very high – patient could be harmed	High	Authenticate all software updates	Acceptable

9.3.2.3 Starting with Assets

Asset	Vulnerability	Impact	Threat	Likelihood	Risk	Mitigating Control	Residual Risk
Patient data	Data sent unencrypted	Medium – patient data exposed	Attacker reads data	Medium	Medium	Encrypted all transmitted data	Acceptable
Patient therapy	No authentication on transmitted data	High – inappropriate therapy	Attacker replays recorded traffic	Medium – requires sophistication	Medium	Authenticate transmissions	Acceptable

The following observations can be made after examining the tables:

1. Analyses starting from consideration of different factors may be identical (see “attacker reads patient data” in 9.3.2.2 and “patient data” in 9.3.2.3. This suggests

that considering the different factors is not necessary. However, starting from the different factors can uncover different risks that might not be considered otherwise. Any combination of the three methods, or one by itself, is acceptable, provided all risks have been considered.

2. There is a need to make a qualitative judgment as to the likelihoods and impacts. This can be difficult for lesser experienced developers. One possible approach is, if in doubt as to the values, then assume a high risk and mitigate. This is the approach taken in the Common Criteria Protection Profiles. It also is appropriate as many of the commonly encountered risks (like a weak or non-existent password policy) and associated mitigations can be considered what TIR57 refers to as basic cyber hygiene [21, p. 55].

9.3.3 TIR57 Basic Cyber Hygiene and Advanced Concepts

These are best practices that should be followed by developers without the need to consider in a risk analysis. Some are listed here:

1. Require unique default passwords to be changed upon first use.
2. Do not hard code passwords.
3. Enforce complex password policies.
4. Use authenticated and encrypted communications.
5. Assign privileges appropriate to a user's authority; manage and control the use of administrator privileges.
6. Authenticate software updates.

These could be enumerated in the security functional requirements (section 9.2.2); item 5 is a restatement of item 4.a in that section. They could also be documented in the design specification document (see item 7.b in section 8.4) along with the mitigating controls developed during the risk analysis.

TIR57 also has recommendations for more advanced security risk controls. These are:

1. Perform final authentication and authorization at the point where any therapy is delivered. For the Kidneato system, this means at the implant. This prevents any compromised software being introduced past the point of last authentication and authorization.
2. Use two way authentication for all communication between all components of the system. This prevents an attacker from masquerading as a legitimate user if the attacker penetrates the system past the point of last authentication.

One example in bConnected that highlights a more advanced risk control method consistent with item 1 is the implementation of access control management. To mitigate the risk of an attacker possibly bypassing the backend server with a direct access to the backend database, bConnected implements the access right closely coupled with its linked data component within the database. The authorization of access is validated upon each data query. This mitigates this specific risk while ensuring the flexibility to provide the proper access right to different users for different components.

These recommendations and risk analysis methods will be employed when considering a risk analysis of the mobile component of bConnected,

9.4 bConnected Mobile Risk Analysis

As a starting point, four existing analyses can be considered:

1. The TIR57 Kidneato system
2. “Protection Profile for Application Software” [50]
3. “Protection Profile for Mobile Device Management” [51]
4. “Protection Profile for Mobile Device Fundamentals” [52]

The use of the Kidneato system was described in 9.3. The use of Protection Profiles in the risk analysis process is considered next.

9.4.1 Use of PPs in bConnected Mobile Risk Analysis

The three Protection Profiles considered for use do not address medical devices, but as described in section 9.3, it is the cybersecurity related functions of the device, not the specific medical functions, that are important in a cybersecurity risk analysis. Additionally, rather than a risk analysis, a PP contains a “Security Problem Description” which discusses threats, and a “Security Objective” which discusses mitigations. In PPs, the assumption is that any threat needs mitigation. A PP also describes considerations for the operational environment. All of this information is useful in a risk analysis. The threats and associated mitigations identified in these PPs are listed in Table 5. Table 6 lists the considerations for the operational environment. Most of the same threats, mitigations and operational environment consideration can be found in all three PPs.

Threat	Mitigation
A threat actor accesses information exchanged between the mobile device and other components	Use a trusted communication path (using HTTPS for example); that is, encrypt all communication
A threat actor conducts a MiTM attack (see 4.4)	Use a trusted communication path (using HTTPS for example)
A threat actor steals the mobile device and accesses the data on it and/or uses the device and its resources as an access point	Use data-at-rest-protection by encrypting data and keys, and authenticate and authorize users when they attempt to access the device
Malicious apps attempt to exfiltrate data or attack other parts of the mobile device and connected system. Flawed apps may allow access to functions that should not be permitted	Self-tests will be performed to ensure the integrity of software and data. A trusted software update method will be used. Access logs of users and apps will be maintained. Whitelisting of trusted apps will be done.

Table 5: PP Threats and Mitigation Applicable to bConnected Mobile

An examination of Table 5 reveals that several of the threats and associated mitigations (encrypt all communications, authenticate and authorize users, use trusted software updates, maintain access logs) have already been discussed either as part of bConnected's Security Functional Requirements (see 9.2.2) or as basic cyber hygiene (see 9.3.3) which will be incorporated in bConnected's design specification. Encrypting data-at-rest can also be considered a basic part of cyber hygiene and so should also be incorporated into the design specification. Self-tests are a function of the mobile device system software; since bConnected Mobile is using a commercial off-the-shelf (COTS) device (as opposed to developing its own mobile device), this should be considered as part of the security characteristics portion of the risk analysis (see sections 7.2 and 9.4.3).

Operational environment assumptions	Rationale
The security functions provided by the mobile device have been properly configured by an administrator	Ensures that the device will function properly from a security perspective. Requiring an administrator to configure the device lessens the possibility of incorrect configuration due to a user's inexperience or ignorance
A user will notify the administrator immediately if the device is lost or stolen	Lessens the possibility of an attacker breaching the system and minimizes damage if a breach has already occurred
The user will take precautions to reduce the risk of theft or loss of the device	See above
The user will use the device and associated app in compliance with any security policies (for example not share authentication information like app passwords or device access codes)	At some level, trust is required for cybersecurity to function
The mobile device hardware and system software provides cybersecure services to the user and the mobile app	This assumption is testable

Table 6: Operational Environment Considerations

An examination of Table 6 reveals that at some point, some element of trust is required to proceed with design activities. For bConnected Mobile, the trust assumption is that the user will act responsibly. The other assumptions can be confirmed by test or inspection.

With these assumptions, the risk analysis for bConnected Mobile can be finalized. The first element to address is intended use.

9.4.2 bConnected Mobile Intended Use

The intended use for the mobile portion of bConnected follows from the intended use statement for the bConnected system (see 9.1.1). It is to aggregate the data from the sensors and transmit the data to the front end. The sensors will communicate over a

Bluetooth link. This link has not yet been considered from a risk perspective (until this point, the secure communication discussion focused on the use of HTTPS, which is not possible for this link). Additionally, the initial design concept (see section 9.2.3, item 4) associated with bConnected mobile's intended use is to allow for clear text storage of sensed data in the event that a connection to the front end is not available. This has to be justified from a risk perspective.

9.4.3 bConnected Mobile Security Characteristics

The hardware portion of bConnected mobile is comprised of COTS equipment. The mobile device must, at a minimum, support the following cybersecurity functions: communication via HTTPS; secure storage of keys and PII; memory integrity self-tests; and, secure Bluetooth connections. The sensors must also support secure Bluetooth connections. These requirements can be used to define acceptance criteria used to select the COTS hardware. The candidate mobile device for bConnected is a Samsung Galaxy tablet running the Android operating system. The test procedures developed for bConnected Mobile (see 9.5) contains tests to verify that this device provides the required functionality.

9.4.4 bConnected Mobile Operational Environment

The operational environment for bConnected mobile is described in Table 6. The administrator will need to install certificates for verifying the authenticity of the front end server, and the source of software updates. This requirement needs to be described in the labelling for bConnected (see section 8.3).

9.4.5 bConnected Mobile Remaining Threats, Vulnerabilities and Assets

As mentioned in section 9.4.2, two issues were uncovered during consideration of the intended use statement for bConnected mobile: Bluetooth connection; and plaintext storage of sensed data. The Bluetooth connection can be considered from the standpoint of any of the three risk factors:

1. threat – attacker uses insecure Bluetooth connection to gain unauthorized access to bConnected mobile
2. vulnerability – insecure Bluetooth connection can be exploited to gain unauthorized access to bConnected mobile
3. asset – Bluetooth connection exists and may allow unauthorized access to bConnected mobile if not properly secured.

Using the vulnerability as the starting point, the following results.

Vulnerability	Likelihood of exploit	Impact	Risk	Mitigating Control	Residual Risk
No authentication on Bluetooth connection	Medium – requires some sophistication to masquerade and reasonably close proximity	High – potentially very high if attacker can gain access to rest of the system	Medium	Authenticate sensor with mobile device	Acceptable

Table 7: Bluetooth Risk Analysis

The plaintext storage of sensed data can be considered from the standpoint of an asset, with its vulnerability being that it is visible by anyone with access to the device, if the device is unlocked either legitimately or illegitimately. Note that the data is visible, but cannot be changed. The risk to patient safety is very low, and since the PII has been stored securely, the risk to privacy is also very low. Therefore, for this scenario, the risk is acceptable as it, without any further mitigation. This illustrates the concept that not all risks need mitigation. A rationale for not pursuing any mitigation is needed, however.

The risk analysis for the bConnected mobile component will need to be revisited as the design progresses in order to address any newly uncovered vulnerabilities and threats. Once the design is mature, then cybersecurity testing can be performed.

9.5 bConnected Testing

The last activity before deployment of bConnected is to perform cybersecurity testing as described in 7.3. Prior to commencement of this testing the following tasks need to be performed:

1. Deployable versions of the various software components need to be created. As part of this, the vulnerability databases should be queried to ensure that any newly discovered and applicable vulnerabilities are appropriately addressed.
2. Test procedures for the various components need to be prepared (see 7.3.2 and 7.3.3).
3. Safety and effectiveness testing should be completed to the degree needed to provide confidence that the final configuration of the system is stable and ready for cybersecurity testing. This prevents having to repeat cybersecurity testing should any deficiencies in system safety and effectiveness be uncovered which result in changes that invalidate the configuration used in the cybersecurity testing.

Because bConnected was still being developed when this document was prepared, actual test results and device labelling are not available. However, a partial test procedure was created, referenced to the requirements described in Table 9 in Appendix A. The procedure should give a developer an idea of the scope and complexity of cybersecurity testing. It is shown below in Table 8.

Health Canada Design Principle	Testing Activities
Secure Communications: • consider how the device will interface with other devices or networks. Interfaces may include hardwired connections and/or wireless communications. • determine the method the device will use to communicate with users (e.g., patients or healthcare professionals), other medical devices/sensors or healthcare systems. Examples of interface	Exercise the device attempting to transmit data while capturing packets from the application (wireshark). Verify from the packet capture that the traffic is encrypted with a secure protocol such as HTTPS, TLS. Verify strong cryptographic algorithms are used. Review the packet capture and verify that no sensitive data is transmitted in the clear.

methods include Wi-Fi, Ethernet, Bluetooth and USB. • consider how data transfer to and from the device will be secured to prevent unauthorized access.	For Android: If "not transmit any data" is selected, ensure that the application's AndroidManifest.xml file does not contain a <uses-permission> or <uses-permission-sdk-23> tag containing android:name="android.permission.INTERNET". Determine whether the application or the platform or both stores sensitive data. Examine filesystem locations where the application may write data. Run the application and attempt to store sensitive data. Inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted. If the application does not store sensitive data determine that sensitive data cannot be written to non-volatile memory. For Android verify that it describes how files containing sensitive data are stored with the MODE_PRIVATE flag set.
Data Security: • consider if data that is stored on or transferred to the device requires some level of encryption. • consider design controls that take into account a device that communicates with a system and/or a device that is less secure (e.g., a device connects to a home network or a legacy device with no device security controls).	Data in transit testing as described above. Data at rest: Inventory the filesystem locations where the application may write data. Run the application and inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted. If the application does not store sensitive data ensure that sensitive data cannot be written to non-volatile memory. If the application leverages platform-provided functionality (Android) verify that files containing sensitive data are stored with the MODE_PRIVATE flag set.
User Access: • user access controls that validate who can use the device. • authentication that grants privileges to different classes of users. • examples of authentication or access authorization include passwords, hardware keys or biometrics.	Check for default passwords. Compose passwords that either meet device requirements, or fail to meet the requirements, in some way. For each password, verify that the device supports the password. Configure the device with the appropriate credential supported for each login method. For that credential/login method, then show that providing correct I&A information results in the ability to access the device, while providing incorrect information results in denial of access.

	Determine that services available are limited to only those authorized. Authenticate to the device. While making this attempt, verify that at most obscured feedback is provided while entering the authentication information. Configure the number of successive unsuccessful authentication attempts allowed by the device (and, if applicable the time period after which access is re-enabled). Test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful. Verify that the application uses the Android KeyStore or the Android KeyChain to store certificates.
Software Maintenance: • consider how the software will be updated to secure the device against newly discovered cybersecurity threats. • consideration should be given to whether updates will require user intervention or be initiated by the device.	Verify that the application provides the ability to check for updates and patches to the application software. Check that the application is packaged in the Android application package (APK) format. The actual installation of any updates could be done by the platform. Record the path of every file on the entire filesystem prior to installation of the application, and then install and run the application. Afterwards, uninstall the application, and compare the resulting filesystem to the initial record to verify that no files, other than configuration, output, and audit/log files, have been added to the filesystem. Install the application and then locate all of its executable files. For each file, save off either a hash of the file or a copy of the file itself. Run the application and exercise all features of the application. Compare each executable file with either the saved hash or the saved copy of the files. Verify that these are identical. Verify that the application installation package and updates to it are signed by an authorized source. Determine how candidate updates are obtained. Perform a version verification activity to determine the current version of the software.

	Obtain a legitimate update and verify that it is successfully installed. After the update, perform the version verification activity again to verify the version correctly corresponds to that of the update and that the current version of the product and most recently installed version match again. Obtain or produce an illegitimate update and attempt to install on the product. Verify that the product rejects all of the illegitimate updates. Check to determine at least the following tests are performed: a) Verification of the integrity of the firmware and executable software. b) Verification of the correct operation of the cryptographic functions.
Hardware and Physical Design: • consider controls to prevent an unauthorized person from making physical and software changes to the device in order to bypass security controls (e.g., disable a USB port that is not being used on device to prevent unauthorized access via USB key).	Perform platform-specific actions to determine the application's access to hardware resources. For each resource which it accesses, identify the justification as to why access is required. Inspect permissions presented at installation time (Android 5.1 and below) or on-access (Android 6.0 and above) for each hardware resource an app intends to access.
Reliability and Availability: • consider design controls that will allow the device to detect, resist, respond and recover from cybersecurity attacks.	Test the products ability to correctly generate audit records by having the product generate audit records. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, events must be generated for each mechanism. Test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols used. Attempt to delete the audit trail in a manner that the access controls should prevent (as an unauthorized user) and verify that the attempt fails. Attempt to modify the audit trail in a manner that the access controls should prevent (as an unauthorized application) and verify that the attempt fails.
Vulnerabilities and Exploits Testing	Port and services scanning Open Source Vulnerability Search Vulnerability Scan Fuzz testing

Software Weakness Testing	Source Code Security Analyzer NIST's list of Source Code Security Analysis Tools

Table 8: Partial bConnected Mobile Test Procedures

References

[1] The Economist newspaper, *“Surgical Intervention”, Feb 3, 2018, pg 53.,* London: The Economist, 2018.

[2] The Economist newspaper, *"Pill Crushers", Feb 3, 2018, pg 54.,* London: The Economist, 2018.

[3] R. Bernhardt and I. Glasgow, *Private Communication, March 19, 2019, Meeting of Technical Report Working Group,* Ottawa: NRC, 2019.

[4] N. Perlroth and D. E. Sanger, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool," 12 May 2017. [Online]. Available: https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?module=inline,%20retrieved%20Jan%2023,%202019. [Accessed 28 January 2019].

[5] White House Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," White House, Washington DC, 2018.

[6] Gov't of Canada, "New Cyber Security Strategy bolsters cyber safety, innovation and prosperity," 12 June 2018. [Online]. Available: https://cyber.gc.ca/en/news/new-cyber-security-strategy-bolsters-cyber-safety-innovation-and-prosperity,retrieved Jan 23, 2019. [Accessed 28 January 2019].

[7] US Federal Register, "Executive Order 13636 - Improving Critical Infrastructure Cybersecurity," 19 February 2013. [Online]. Available: https://www.gsa.gov/cdnstatic/ATTCH_1_-_CyberEO-FedReg.pdf, retrieved Jan 23, 2019. [Accessed 28 January 2019].

[8] Govt of UK, "Chancellor announces new National Cyber Centre in speech at GCHQ," 16 Nov 2015. [Online]. Available: https://www.ncsc.gov.uk/news/chancellor-announces-new-national-cyber-centre-speech-gchq. [Accessed 28 January 2019].

[9] ""Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis”, FDA Workshop, Transcript of meeting, May 18-19, 2017," 18 May 2017. [Online]. Available: https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm549732.htm. [Accessed 28 January 2019].

[10] "Notice: Health Canada's Approach to Digital Health Technologies," 10 April 2018. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-digital-health-technologies.html. [Accessed 28 January 2019].

[11] Health Canada, "Scientific Advisory Committe on Digital Health Technologies," 8 June 2018. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/scientific-expert-advisory-committees/digital-health-technologies/terms-reference-2018-05-28.html. [Accessed 28 January 2019].

[12] Health Canada, "Scientific Advisory Committe on Digital Health Technologies -Question," 6 December 2018. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/scientific-expert-advisory-committees/digital-health-technologies/questions.html. [Accessed 28 January 2019].

[13] Health Canada, "Draft Guidance Document - Premarket Requirements for Medical Device Cybersecurity," 7 December 2018. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/public-involvement-consultations/medical-devices/consutation-premarket-cybersecurity-profile/draft-guidance-premarket-cybersecurity.html. [Accessed 7 December 2018].

[14] CSE, "What we do and why we do it," 7 February 2018. [Online]. Available: https://www.cse-cst.gc.ca/en/inside-interieur/what-nos. [Accessed 28 January 2019].

[15] CSE, "Common Criteria," 30 September 2018. [Online]. Available: https://cyber.gc.ca/en/common-criteria. [Accessed 28 January 2019].

[16] NRC, "100 years of innovation for Canada," 20 July 2017. [Online]. Available: https://www.nrc-cnrc.gc.ca/eng/about/centennial/100_years/1946_1964.html. [Accessed 28 January 2019].

[17] IEC, "Medical Device Software - Software Life Cycle Processes, Ed 1.1," International Electrotechncial Commission / International Standards Organization, Geneva, 2015.

[18] ISO, "Medical devices — Application of risk management to medical devices," International Organization for Standardization, Geneva, 2007.

[19] ISO, "Medical devices -- Quality management systems -- Requirements for regulatory purposes," International Organization for Standardization, Geneva, 2016.

[20] Underwriters Laboratories, "UL Consumer Technology Knowledge Center," [Online]. Available: https://ctech.ul.com/wp-content/uploads/2017/07/SS_IoTSecurityTop20_0117.pdf. [Accessed 30 July 2018].

[21] Assocation for the Advancement of Medical Instrumentation (AAMI), "Technical Information Report (TIR) 57:2016 Principles for medical device security - Risk management," Association for the Advancement of Medical Instrumentation (AAMI), 2016.

[22] C. Ault, "The Top 5 Things You Need To Know Before Adding Connectivity to Your Medical Device," 8 Dec 2015. [Online]. Available: http://blackberry.qnx.com/en/news/web_seminars/The_Top_5_Things_You_Need_To_Know_Before_Adding_Connectivity_to_medical_device. [Accessed 12 Dec 2015].

[23] A. Arbelaez, R. Daldos, S. Wang and D. Weitzel, "Securing Telehealth Remote Patient Monitoring Ecosystem - Draft," November 2018. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-draft.pdf. [Accessed November 2018].

[24] R. A. Grimes, ""Hacking the hacker: learn from the experts who take down hackers", chapter 45 "Patching Facts"," [Online]. Available: http://common.books24x7.com/toc.

[25] R. L. Rivest, "Cryptography," in *Handbook of Theoretical Computer Science. 1*, New York, Elsevier, 1990.

[26] W. R. Stevens and K. R. Fall, TCP/IP Illustrated, Volume 1: The Protocols, Second Edition, Upper Saddle River NJ: Pearson Education, 2012.

[27] National Institute of Standards and Technology, "FIPS 197, Advanced Encryption Standard (AES) - NIST Page," 26 November 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf. [Accessed 9 April 2019].

[28] RFC Editor, "Request for Comment 3447," February 2003. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3447.txt. [Accessed 9 April 2019].

[29] B. Kaliski, "Twirl and RSA Key Size," RSA Laboratories, 6 may 2003. [Online]. Available: https://web.archive.org/web/20170417095741/https://www.emc.com/emc-plus/rsa-labs/historical/twirl-and-rsa-key-size.htm. [Accessed 9 April 2019].

[30] Communications Security Establishment, "CMVP," Communications Security Establishment, 23 June 2017. [Online]. Available: https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program. [Accessed 9 April 2019].

[31] Canadian Centre for Cyber Security, "Cyber Threat and Cyber Threat Actors," Canadian Centre for Cyber Security, 6 December 2018. [Online]. Available: https://www.cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors. [Accessed 11 April 2019].

[32] CVE, "CVE List Home," Mitre, [Online]. Available: https://cve.mitre.org/cve/. [Accessed 30 January 2019].

[33] National Institute for Standards and Technology, "National Vulnerability Database," NIST, [Online]. Available: https://nvd.nist.gov/. [Accessed 31 Jan 2019].

[34] Mitre, "Common Weakness Enumeration," Mitre, 3 April 2018. [Online]. Available: https://cwe.mitre.org/index.html. [Accessed 27 February 2019].

[35] First, "Common Vulnerability Scoring System SIG," First.org, [Online]. Available: https://www.first.org/cvss/. [Accessed 27 Februray 2019].

[36] F. Donovan, "Qualcomm's Medical Gateway Has Critical Cybersecurity Vulnerability," HealthITSecurity, 29 August 2018. [Online]. Available:

https://healthitsecurity.com/news/qualcomms-medical-gateway-has-critical-cybersecurity-vulnerability. [Accessed 1 September 2018].

[37] DHS, "Advisory (ICSMA-18-240-01)," ICS-CERT, 28 August 2018. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-18-240-01. [Accessed 1 Sept 2018].

[38] Mitre, "Search Results," Mitre, [Online]. Available: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2014-9222+. [Accessed 27 February 2019].

[39] Mitre , "Search Results," Mitre, [Online]. Available: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2014-9223. [Accessed 27 February 2019].

[40] Allegro Software, "Allegro Software Urges Manufacturers," 19 December 2014. [Online]. Available: https://www.allegrosoft.com/allegro-software-urges-manufacturers-to-maintain-firmware-for-highest-level-of-embedded-device-security/news-press.html. [Accessed 1 September 2019].

[41] H-ISAC, "H-ISAC FAQ," H-ISAC, 2018. [Online]. Available: https://h-isac.org/h-isac-faq/. [Accessed 27 February 2019].

[42] CCTX, "CCTX," CCTX, 2019. [Online]. Available: https://cctx.ca/. [Accessed 2 April 2019].

[43] NIST, "NIST Cybersecurity Framework," NIST, [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 8 August 2018].

[44] Food and Drug Administration, "Cybersecurity," 18 October 2018. [Online]. Available: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf. [Accessed 1 November 2018].

[45] CSE, "IT Security Risk Management: A Lifecycle Approach," November 2012. [Online]. Available: https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33. [Accessed 15 May 2019].

[46] R. Bernhardt and C. Clark, *Private Communication,* Winnipeg/Ottawa: NRC, February 2019.

[47] Underwriters Laboratories, "UL 2900-1, "Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements"," Underwriters Laboratories, Chicag0, 2017.

[48] Underwriters Laboratories, "UL 2900-2-1 “Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems," Underwriters Laboratories, Chicago, 2017.

[49] Underwriters Laboratories, "Mapping cybersecurity standards to FDA guidance," Underwriters Laboratories, Chicago, 2017.

[50] NIAP, "Protection Profile for Application Software," 22 April 2016. [Online]. Available: https://www.niap-ccevs.org/MMO/PP/-394-/pp_app_v1.2.htm. [Accessed 20 August 2018].

[51] NIAP, "Protection Profile for Mobile Device Management," 31 December 2014. [Online]. Available: https://www.niap-ccevs.org/MMO/PP/pp_mdm_v2.0.pdf. [Accessed 20 August 2018].

[52] NIAP, "Protection Profile for Mobile Device Fundamentals," 16 June 2017. [Online]. Available: https://www.niap-ccevs.org/MMO/PP/pp_md_v3.0.pdf. [Accessed 20 August 2018].

[53] NIAP, "US Government Approved Protection Profile - collaborative Protection Profile for Network Device," 14 March 2018. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=422&id=422. [Accessed 1 January 2019].

[54] IEC, "Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities," International Organization for Standardization, Geneva, 2010.

[55] UK Department for Digital, Culture, Media and Sportr, "https://www.gov.uk/government/publications/secure-by-design," 2018. [Online]. Available: https://www.gov.uk/government/publications/secure-by-design. [Accessed 30 August 2018].

[56] UK Department, "Code of Practice for Consumer Internet Security," 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf. [Accessed 30 August 2018].

[57] L. Tanczer, J. Blythe, F. Yahya, I. Brass, M. Edsen, J. Blackstock and M. Carr, "Summary literature review of industry recommendations and international developments on IoT security," PETRAS, London.

[58] R. Piggin, "Cybersecurity of medical devices," [Online]. Available: https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf. [Accessed 17 August 2018].

[59] Healthcare and Public Health Sector Coordinating Councils, "The Joint Security Plan," January 2019. [Online]. Available: https://healthsectorcouncil.org/the-joint-security-plan/. [Accessed 14 February 2019].

[60] G. O'Brien, N. Lesser, B. Pleasant, S. Wang, Z. Kangmin, C. Bowers and K. Kamke, "NIST SP1800-1 "Securing Electronic Health Records on Mobile Devices"," July 2018. [Online]. Available: https://www.nccoe.nist.gov/projects/use-cases/health-it/ehr-on-mobile-devices. [Accessed 1 March 2019].

[61] G. O'Brien, S. Edwards, K. Littlefield, N. McNab, S. Wang and Z. Kangmin, "SP1800-8 "Securing Wireless Infusion Pumps"," August 2018. [Online]. Available: https://www.nccoe.nist.gov/projects/use-cases/medical-devices. [Accessed 13 March 2019].

[62] OWASP, "OWASP Main page," OWASP, 25 March 2019. [Online]. Available: https://www.owasp.org/index.php/Main_Page. [Accessed 11 April 2019].

[63] M. Meucci and A. Muller, "OWASP Testing Project," 8 February 2017. [Online]. Available: https://www.owasp.org/index.php/OWASP_Testing_Project. [Accessed 20 March 2019].

[64] Standards Council of Canada, "Software development and cybersecurity evaluation program," Standards Council of Canada, 2019. [Online]. Available: https://www.scc.ca/en/standards/notices-of-intent/csa/software-development-and-cybersecurity-evaluation-program. [Accessed 18 April 2019].

[65] Tenable, "Tenable Nessus Professional," Tenable, [Online]. Available: https://www.tenable.com/products/nessus/nessus-professional. [Accessed 28 February 2019].

[66] OpenVAS, "OpenVAS - Open Vulnerability Assessment System," OpenVAS, [Online]. Available: http://openvas.org/. [Accessed 28 February 2019].

[67] Nmap, "Nmap," Nampo, [Online]. Available: https://nmap.org/. [Accessed 28 February 2019].

[68] Rapid 7, "Rapid7 Nexpose," Rapid 7, [Online]. Available: https://www.rapid7.com/products/nexpose/. [Accessed 28 February 2019].

[69] Wireshark.org, "Wireshark," Wireshark, [Online]. Available: https://www.wireshark.org/. [Accessed 28 February 2019].

[70] TCPDump, "TCPDump&LibCap," TCPdump, [Online]. Available: https://www.tcpdump.org/. [Accessed 28 February 2019].

[71] Rapid 7, "Rapid 7 Metasploit," Rapid 7, [Online]. Available: https://www.metasploit.com/. [Accessed 28 February 2019].

[72] Scapy, "Scapy," Scapy, [Online]. Available: https://scapy.net/. [Accessed 28 February 2019].

[73] getfirebug, "Firebug," Getfirebug, [Online]. Available: https://getfirebug.com/. [Accessed 28 February 2019].

[74] ettercap project, "ettercap home page," ettercap, [Online]. Available: https://www.ettercap-project.org/. [Accessed 28 February 2019].

[75] PeachTech, "PeachTech," PeachTech, [Online]. Available: https://www.peach.tech/. [Accessed 28 February 2019].

[76] Sourceforge, "Taof - The art of fuzzing," Sourceforge, [Online]. Available: https://sourceforge.net/p/taof/wiki/Home/. [Accessed 28 February 2019].

[77] R. Bernhardt, *Notes from the meeting between NRC MD & DT, CSE, and Health Canada (HC), May 30, 2018, at Bldg M-55,* Ottawa: NRC, 2018.

[78] K. Hoyme, "Developing a ‘Software Bill of Materials’ for the Future of Cybersecurity," AAMI, 2 October 2018. [Online]. Available: https://aamiblog.org/2018/10/02/ken-hoyme-developing-a-software-bill-of-materials-for-the-future-of-cybersecurity/. [Accessed 29 January 2019].

[79] FDA, "Public Workshop - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices January 29-30, 2019," Food and Drug Administration, 04 February 2019. [Online]. Available: https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm623171.htm. [Accessed 6 February 2019].

[80] Dr. Dobb's, "Implementing a Version Description Document," 1 January 1996. [Online]. Available: http://www.drdobbs.com/implementing-a-version-description-docum/184415521. [Accessed 29 January 2019].

[81] R. DiRaddo, "Healthcare delivery soaring to new heights with interactive simulation," Research Features, 31 October 2016. [Online]. Available: http://researchfeatures.com/2016/10/31/interactive-simulation/. [Accessed 27 February 2019].

[82] M. Jones, J. Bradley and N. Sakimura, "JSON Web Token," Internet Engineering Task Force, May 2015. [Online]. Available: https://tools.ietf.org/html/rfc7519. [Accessed 7 May 2019].

[83] National Institute for Standards and Technologies, "NIST SP 800-30 Rev 1,Guide for Conducting Risk Assessments," September 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. [Accessed 2 May 2019].

[84] Comptroller and Auditor General,, "Investigation: WannaCry cyber attack and the NHS," UK National Audit Office, London, 2018.

Appendix A

Health Canada Design Principles (from Table 1 of Pre-market Guidance document)	UL Top 20 List	Common Criteria Protection Profiles	PETRAS Summary	Secure by Design Code of Practice
Secure Communications: • how will the device interface with other devices or networks (eg. Hardwired, wireless, combination, using what protocol or software stack)? • how will the device communicate with users, other medical devices/sensors or healthcare systems? • how will data transferred to and from the device be secured?	Use industry standard security protocols for any remote or wireless connections - #5	*Application Software*[1] - Protection of Data in Transit FTP_DIT_EXT.1.1[2]	Cryptographic Protocols and Best Practices	Communicate Securely - #5 Securely Store Credentials and Security Sensitive Data - #4
Data Security: • does data stored on or transferred to the device require encryption? • how will a device communicate with a system and/or device that is less secure (e.g., one on a home network or an unsecured legacy device)?	Do not store passwords in clear text - #6	*Application Software* - Encryption of Sensitive Application Data FDP_DAR_EXT.1	Cryptographic Protocols and Best Practices	Communicate Securely - #5 Ensure that personal data is protected - #8
User Access: • use user access controls that validate who can use the device. • use authentication that grants privileges to different classes of users. • examples of authentication or access authorization include passwords, hardware keys or biometrics.	Implement 'least privilege' - #16	*Network Devices*[3] – Identification and Authentication, Authentication Failure Handling FIA_AFL.1 *Application Software* – Storage of Credentials FCS_STO_EXT.1	Strong Authentication	Securely Store Credentials and Security Sensitive Data - #4 Principle of least privilege - #6
Software Maintenance: • how will the software be updated? • will updates require user intervention or be initiated by the device?	Allow for software updates - #4	*Network Devices* – Trusted Update and Self-tests FPT_TUD_EXT.1[4] *Application Software* – Installation and Update FPT_TUD_EXT.1[4]	Software Updates Secure Device Boot	Keep software updated - #3 Ensure Software Integrity - #7
Hardware and Physical Design: • how to prevent an unauthorized person from making physical and software changes to the	Do not allow for externally provided commands… - #18	*Application Software* – Access to Platform Resources FDP_DEC_EXT.1	Device Functionality	Minimise exposed attack surfaces - #6

device in order to bypass security controls				
Reliability and Availability: • how will the device detect, resist, respond and recover from cybersecurity attacks.		*Network Devices* – Audit FAU_GEN.1	Logging	
1. Application Software refers to Protection Profile for Application Software 2. This is a vernacular specific to PPs. It basically an identifying label. The "F" means it is a functional requirement. 3. Network Devices refers to collaborative Protection Profile for Network Devices. 4. Notice that the same functional requirement is called out in both Protection Profiles.				

Table 9: Requirements Check List

Appendix B

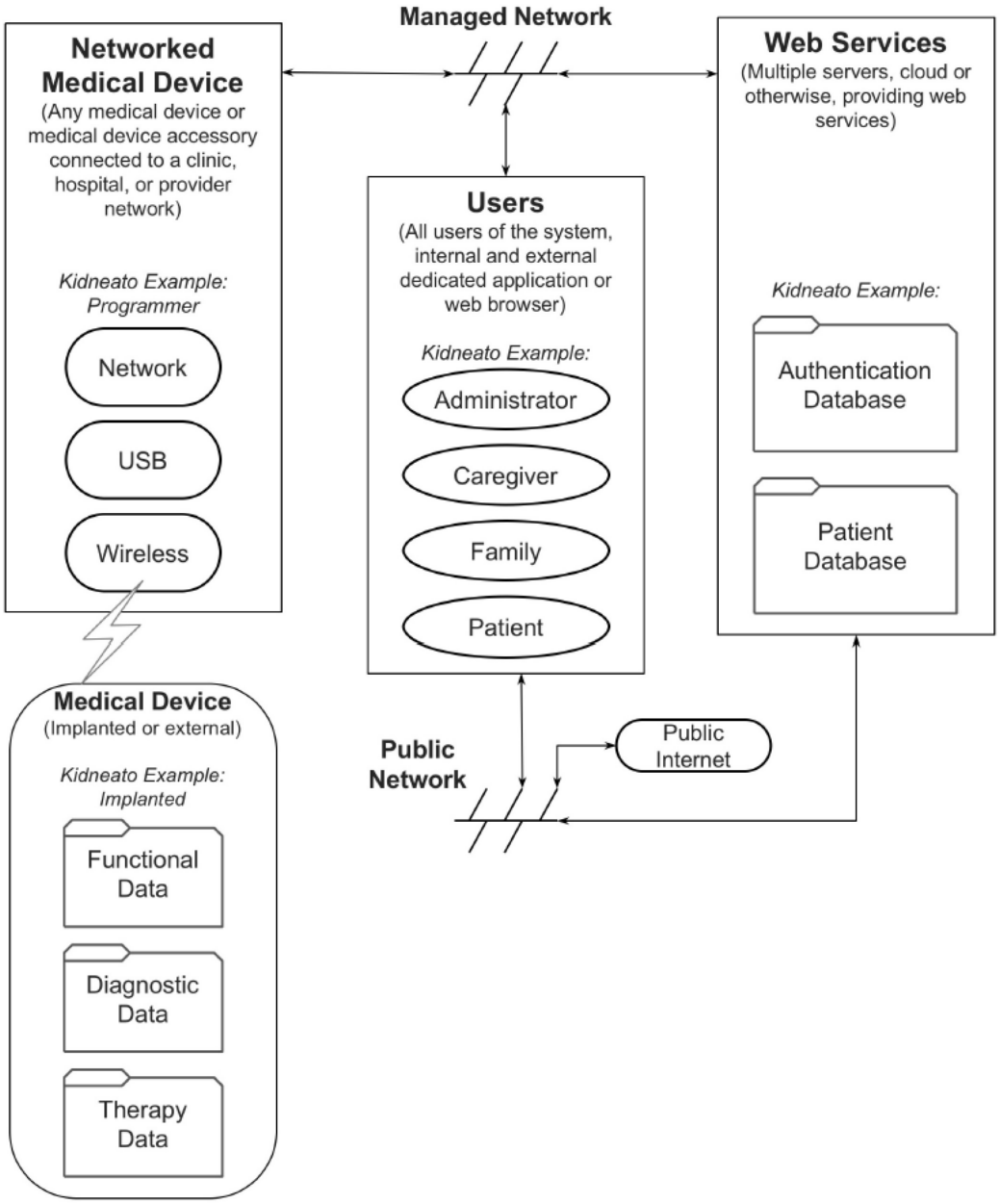

Figure 2: Block Diagram of the Kidneato system, managed environment

Source: [TIR57]. Reprinted with permission from the Association for the Advancement of Medical Instrumentation, Inc.

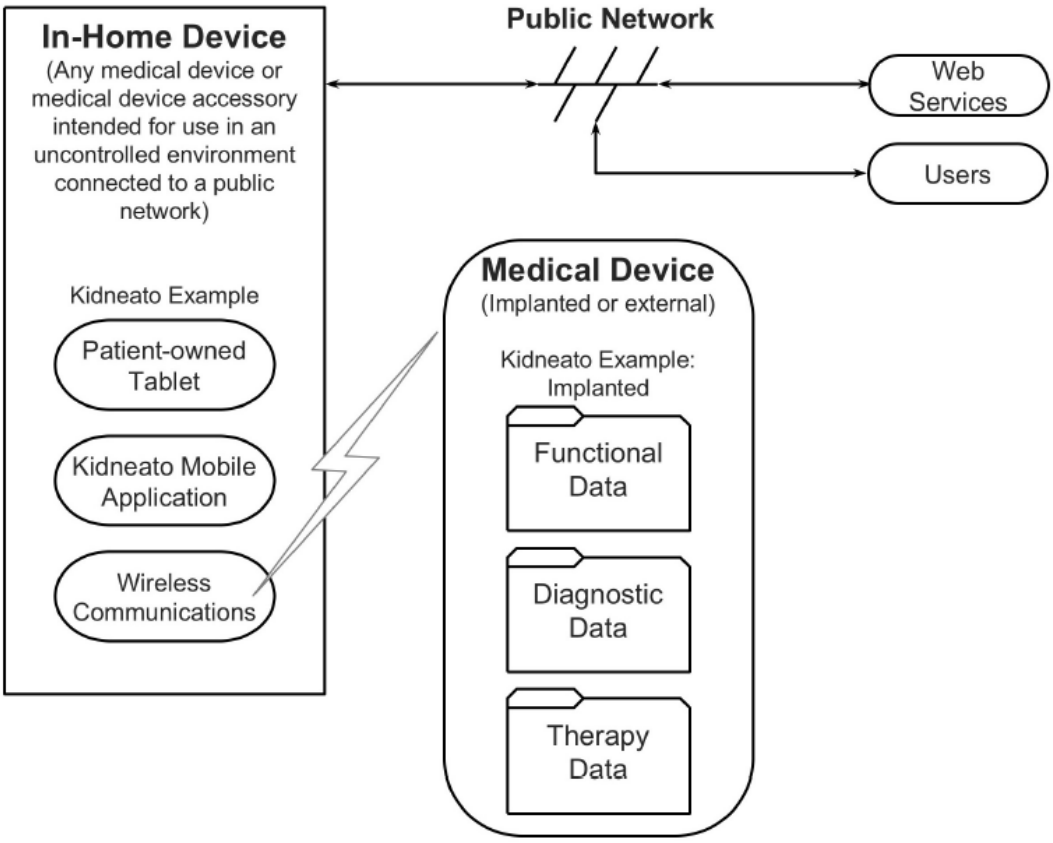

Figure 3: Block diagram of the Kidneato system, patient environment

Source: [TIR57]. Reprinted with permission from the Association for the Advancement of Medical Instrumentation, Inc.