Security Benchmarks for Wearable Medical Things: Stakeholders-Centric Approach

Swapnika Reddy Putta, Abdullah Abuhussein, Faisal Alsubaei, Sajjan Shiva and Saleh Atiewi

Abstract Internet of Medical Things (IoMT) is a fast-emerging technology in healthcare with a lot of scope for security vulnerabilities. Like any other Internet-connected device, IoMT is not immune to breaches. These breaches can not only affect the functionality of the device but also impact the security and privacy (S&P) of the data. The impact of these breaches can be life-threatening. The proposed methodology used a stakeholder-centric approach to improve the security of IoMT wearables. The proposed methodology relies on a set of S&P attributes for IoMT wearables that are identified to quantify S&P in these devices. This work aimed to (1) Guide hesitant users when choosing a secure IoMT wearable device, (2) Encourage healthier competition among manufacturers of IoMT wearables, and therefore, (3) Improve the S&P of IoMT wearables.

Keywords IoT (Internet of Things) · IoMT (Internet of Medical Things) · Wearable devices · Sensors · Security · Privacy · Healthcare

S. R. Putta · A. Abuhussein (✉)
St. Cloud State University, St. Cloud, MN, USA
e-mail: aabuhussein@stcloudstate.edu

S. R. Putta
e-mail: sputta@stcloudstate.edu

F. Alsubaei · S. Shiva
The University of Memphis, Memphis, TN, USA
e-mail: flsubaei@memphis.edu

S. Shiva
e-mail: sshiva@memphis.edu

S. Atiewi
Al Hussein Bin Talal University, Ma'an, Jordan
e-mail: saleh@ahu.edu.jo

X.-S. Yang et al. (eds.), *Fourth International Congress on Information and Communication Technology*, Advances in Intelligent Systems and Computing 1027, https://doi.org/10.1007/978-981-32-9343-4_32

1 Introduction

Internet of Medical Things (IoMT) wearables are Internet-connected electronic devices that can be worn on the body to improve patient's quality of medical treatments. These devices are available from head to toe in many forms such as smart wristbands, watches, eyeglasses, belts, necklaces, patches, etc. They can track physical activity, temperature, glucose, sleep, heart rate, and much more. These devices can monitor the health signs of the patients/users and send them wirelessly to the physicians to cut down personal visits. The use of IoMT wearables is increasing rapidly, and the global wearable medical device market is anticipated to reach an estimated $9.4 billion by 2022 [1].

Although this radical change is much appreciated, we need to take a step back to review the security and privacy (S&P) of such devices. Ensuring their S&P is very important because the consequences of insecure medical devices are very dire as many patient's lives depend on them. Due to the rush to embrace IoMT technologies, the S&P of these devices are often overlooked by manufacturers. While shopping for the IoMT wearables, customers also often focus on the design, price, and performance of these devices. This is because customers are unable to choose or rank these devices in terms of S&P. Also, different stakeholders have different objectives and tolerance for risks. Hence, this work aims to assist hesitant users to evaluate and select IoMT wearables based on their ability to protect customers from potential S&P issues. This work also encourages healthier competition among manufacturers of IoMT wearables and therefore helps to improve the security of IoMT wearables.

2 Related Work

Many researchers and manufactures of IoMT devices are concentrating on the S&P of these medical devices. Also, many regulatory authorities have recognized the importance of this problem and started serious steps toward ensuring the protection of patient health information and the compliance of medical devices. However, the main gaps in these efforts can be summarized as follows: (1) Considering S&P attributes that are specific to a set of IoMT scenarios (e.g., patient monitoring) [2, 3]. (2) Providing generalized S&P recommendations that target manufacturers and considering whole IoMT ecosystems and all IoMT device types [4–8]. (3) Lacking an evaluation method that helps adopters to quantify and compare the S&P of potential IoMT wearables [9–11]. (4) Focusing only on assessing existing IoMT devices by utilizing post-adoption parameters such as configurations and current users' feedback, which requires technical knowledge that often most IoMT stakeholders lack [2, 7, 12].

Even though these works are considered necessary, these works lack methods of measuring security and do not integrate easily into an effective evaluation method for IoMT. Complementing the previous works, this paper presents a method for

measuring S&P in IoMT wearables. The contribution of this paper is a list of S&P evaluation attributes for the IoMT wearables as well as an easy-to-use evaluation method that measures the S&P in IoMT wearables. Our presented solution is designed to help users compare candidate IoMT wearables in terms of their S&P levels in order to make well-informed decisions such as, choosing, or replacing current, IoMT wearables.

3 Wearable IoMT Security Evaluation

Evaluating the S&P in IoMT wearables is *multiple criteria decision-making* problem, which considers multiple conflicting criteria for decision-making. In order to solve this problem, key attributes that are critical for the S&P of IoMT wearables are identified in this work. Each of these attributes is represented by its definition (i.e., what is it?), its rationale (i.e., why is it important?), and its S&P functionality (i.e., how is it important?). Furthermore, each attribute is represented by a set of considerations. These considerations are a set of polar questions (i.e., yes/no questions). The attributes and their considerations are explained in the next chapter.

These attributes along with their considerations are integrated in a two-step methodology to assist the stakeholders when choosing of IoMT wearables. This steps of methodology are as follows:

- **Step 1**: The S&P of IoMT wearables are evaluated by answering the attribute questions. Device S&P specifications can be used by stakeholders to answer these questions. These specifications are publicly available on manufacturers' websites.
- **Step 2**: The score of each attribute is computed using its considerations. The scores for all the attributes are normalized to a score of 10.

Every stakeholder's interaction with the device is different. Hence, not all the attributes are necessary for all the stakeholders. This stakeholder-centric approach helps to satisfy the requirements of the stakeholders who have different needs, goals, and tolerance to risks. The identified stakeholders for these devices include the patient, doctor, hospital, nurse, manufacturer, security researcher, and regulatory authorities, and insurance.

4 IoMT Wearable S&P Attributes

This section discusses our identified S&P attributes. We investigated the attributes that define the S&P of the wearable IoMT devices using devices specification, FAQs and best practices in medical IoMT from research organizations, government agencies, and industry associations. Our attributes are discussed in the following subsections.

4.1 Authentication and Identity Management

This measures the device ability to verify the user identity. Identity is associated with a user with a unique username or unique ID. Authentication verifies the identity of the user with a password or a key. This attribute is important because it defines the effectiveness in protecting device and user data from unauthorized access. The following questions are used to determine the strength of the authentication and identity management of a wearable device:

1. Does the device allow MFA?—Multi-factor authentication (MFA) is a combination of two or more types of authentication. It is always harder to bypass multi-layer security than single-layer security.
2. Is the minimum size of password eight characters?—Recommendations for a minimum length of the password is eight.
3. Does the password require each of uppercase/lowercase/number/special characters?—A strong password is a combination of all the different types of characters.
4. Does the device password expire?—Users should change their passwords regularly at least for every 90 days and they should be notified to do so before they expire.
5. Does the device have a password recovery option?—It is always important to have a password recovery option and to identify the user before resetting the password.
6. Does the device have a password history option?—A password history stores the previous passwords and prevents the same password to be re-used.
7. Does the device have biometric authentication?—Biometric methods use a physical characteristic such as fingerprint, retina, iris, voice recognition or facial recognition.
8. Does the device allow to choose the same password as your username?—setting the same password as your username can be easily guessed by any hacker. The device should display an error message if the user picks a password similar to username.

4.2 Access Control and Profiling

This measures the device ability to grant access and privileges to the resources for the users. These resources can be data, applications, or the device. This access is defined by the permissions assigned based on the authorization to the data and the device. It also measures the ability to define and customize profiles of the users. This helps device owners to limit the access to the device and the privileges that each user has. Only the owner of the device (e.g., patient) should have the highest privilege. The strength of access control and profiling can be determined by the following questions:

1. Does the wearable device have role-based access control?—Role-based access control uses roles to grant/deny permissions. The stakeholders can be categorized by their roles so that a stakeholder has all the necessary privileges for the role.
2. Does the device have rule-based access control?—Rule-based access control uses rules. These rules typically remain static until changed by device owner.
3. Does the device have discretionary access control?—In discretionary access control, the device owner decides and grants access to the other stakeholders.
4. Does the device have mandatory access control?—mandatory access control uses labels (e.g., data sensitivity or security labels) to determine access.
5. Does the device have attribute-based access control?—Attribute-based access control evaluates attributes and grants access based on the value of these attributes.

4.3 Storage Location

This attribute measures the device ability to store data in a secure location(s). Data storage locations include cloud storage, mobile storage, and device storage. This helps the user to recognize the locations where the data is stored so that the user can limit storage locations. Storing the data in multiple locations helps to backup data in redundant locations. However, it also expands the attack surface. A good storage location(s) attribute can be defined by the following questions:

1. Does the device allow the user to store the data in the device itself?—Data stored in the device is easily accessible and can be tracked easily since the device is always worn on the user's body.
2. Does the device allow the user to manage, and control the device data from the device itself?—Since the device is a wearable device and is worn on the body, it is more secure as the device, and the data can be controlled from the device itself.
3. Can users store, access, manage and control the device using a smartphone?—Wearable medical device that can be controlled and managed by the smartphone, can also be accessed by anyone and/or other applications that have access to it.
4. Can users store, access, manage and control the device from cloud/third party apps?—Most of the cloud applications are in the control of a third party. If these applications are hacked and if the device can be managed from these applications, the hacker can easily control the device on the patient's body.
5. Does the device allow the user to select the locations where the data can be stored?—Storing the data in cloud/third parties is always at risk. Users should be able to decide the storage location depending on the requirements and security.

4.4 Encryption

This measures the device ability to make the data unreadable at various levels like data at rest, in transit, and in use. Data can only be read by the user who has the encryption key which converts data to clear text. This attribute guarantees the confidentiality of the patient's data. If data is stored in plain text, it can be read by intruders during the data transmission or while the data is being processed. A good encryption attribute can be defined using the following questions:

1. Does the device allow users to select what data to encrypt and where?—Although encryption guarantees data confidentiality, it consumes time and space. Hence, the customer should be given an option to encrypt only sensitive data to reduce the time and space.
2. Does the device encrypt and hash passwords?—Passwords are usually stored in plaintext in these devices. If the passwords are stored in plaintext, anyone who has access to the device can easily read the password.
3. Does the device encrypt the data at rest?—Data at rest is when the data is not being used but is stored physically on the device, smartphone, and or cloud. If data is not encrypted when it is at rest, the data can be easily viewed if the device is lost/stolen.
4. Does the device encrypt data in transit?—Data in transit is when the data is being transmitted from one location to the other. If data is being communicated in clear text between the two devices, it can be read by eavesdropper.
5. Does the device encrypt data in use?—Data should be encrypted even when it is being used by the device or applications because it helps to protect sensitive data.
6. Does the device follow any of the standard encryption techniques?—There are encryption standards that are proven to be immune to attacks or very hard to be broken.
7. If yes, Does the device comply with regulations in the country where it is used?—Every country has its own laws and regulations to be followed. It is also necessary for the user to check if the device complies with the regulations in the country where the device is being used.
8. Does the device allow the user to choose an encryption technique?—There are different encryption technologies available depending on time and reliability.

4.5 Compliance

Compliance attribute measures the device ability to follow the guidelines set by the regulatory authorities which this increases the trustworthiness of the device. A good compliance attribute can be determined using the following questions:

1. Is the device FDA compliant?—Food and Drug Administration (FDA) is a federal agency of the United States Department of Health and Human Services which is responsible for protecting and promoting public health.
2. Is the device HIPAA compliant?—"Health Insurance Portability and Accountability Act of 1996 (HIPAA) is United States legislation that provides data privacy and security provisions for safeguarding medical information."
3. Is the device ISO/IEC 80001 compliant?—International Organization for Standardization (ISO)/IEC 80001 is application of risk management for IT-networks incorporating medical devices. The key properties are risk management of IT-networks incorporating medical devices to address safety, effectiveness and system security.
4. Is the device ISO 14971 compliant?—ISO 14971:2007 specifies a process for a manufacturer to identify the hazards associated with medical devices, including in vitro diagnostic medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls.
5. Is the device compliant with any other medical device regulatory?—There are different regulations and authorities for medical data and security.
6. Is the device compliant with any regulatory authority where the device is manufactured?—Different authorities have different guidelines based on the location and rules. The device should be compliant to the regulations of manufacturer location.
7. Is the device compliant with any regulatory authority where the device is used?—Different bodies have different guidelines based on the location and rules. The device should be compliant to the regulatory where it is being used.

4.6 Connectivity

This attribute measures the device ability to connect to other devices through a different medium. It defines how the device can be connected to the other devices. Each method of connectivity has its own security challenges. Secure connectivity is determined by the following questions:

1. Does the device allow to select the type of connectivity?—A user might feel comfortable using connectivity methods. Hence, the device should allow the user to choose how to connect to the Internet or the other devices.
2. Does the device allow to connect with other devices via the Internet?—Internet helps to connect and view data in different devices globally. It helps the user to view, edit and share data at any time through the private network. Connecting to the Internet in public places increases hackers' chances to gain unauthorized access to the devices.
3. Does the device have the ability of mutual authentication when connecting with other devices?—Mutual authentication is a two-way authentication that helps both the devices to authenticate before they connect to each other.

4. Can the device anonymously connect to other devices?—Being anonymous can make the user feel safer even when device is breached.

4.7 Data Shredding

This measures the device ability to ensure that all patient identifiable data is securely and correctly deleted from the equipment prior to disposal or reuse. It ensures that the device does not retain previous user's data or malicious code. Data shredding permanently wipes data so that it cannot be recovered. A good data shredding attribute can be defined by the following questions:

1. Is the device under MDISS agreement?—Medical Device Innovation, Safety and Security (MDISS) consortium checks if the medical device is ready to use, no previous data is present in the device, and helps the device to fix any vulnerabilities.
2. Does the device use any data shredding mechanisms?—Data shredding mechanisms help the medical devices to clear all data that was previously stored by other users.
3. Is the device capable of installing any data shredding tools?—There are many open-source data shredding tools that help to wipe all the previously stored data.

4.8 Classification of Data

This attribute helps to determine the type of data that is stored in the device and helps to categorize the data depending on its sensitivity. The more sensitive data on the device, the more risk it introduces if device hacked. This can be verified by the following questions:

1. Does the device allow to catalog, categorize or classify data based on their sensitivity?—Categorizing the data helps the user to know which data can be encrypted.
2. Does the device allow the owner to select the validity for the data stored in the device?—A user can delete the less important data after a period of time which helps the device to increase the storage space and helps to improve the processing time.

4.9 Simultaneous Data Accessed

This attribute measures the device ability to access the data by different users/programs at the same time. It is vital because data accessed at the same time by different users/programs increases the attack surface. This is measured by the following questions:

1. Can the device restrict multiple users from connecting to the device at the same time?—Each device can have different users. If all the users connect at the same time, the functionality of the device decreases, and it also becomes hard to track attacks.
2. Does the device have an option to limit the number of users accessing the device at the same time?—If the user can restrict the connections to the device, it helps to track the user or the program if the device is compromised.

4.10 Number of Stakeholders

This measures the device ability to identify how many users can have access to the data and who they are. As the number of stakeholders increases the attack surface also increases. This is measured by the following questions:

1. Does the device allow the owner to select the users?—The owner of the device should have the privilege to choose the users.

4.11 Device Bandwidth

This measures the device ability to control communication bandwidth. Bandwidth is measured in bits per second. If the traffic exceeds the allowed bandwidth threshold that may possibly mean that the device under a denial of service attack. To verify this attribute, the following questions can be used:

1. Does the device allow the owner/admin to limit the bandwidth?—Bandwidth should be limited based on the data that is being transmitted.
2. Does the device allow the owner to limit the bandwidth for different users?—There are different bandwidth recommendations for healthcare users such as the federal communication commission recommendations [13].
3. Does the device allow the user to limit the bandwidth based on the number of users?—There might be situations where the number of users accessing the device at the same time increases, at that time the device should allow the owner/admin to increase the bandwidth depending on the number of stakeholders.

4. Does the device allow owner/admin to limit bandwidth based on the user locations?—There might be unwanted traffic in public networks, so depending on the location, the bandwidth should be limited.

4.12 Tested Device

This attribute measures if the device is tested and all its vulnerabilities are addressed. This helps to determine the current level of security of the device, the device vulnerabilities and if they were patched? This can be defined by the following questions:

1. Is the device tested in terms of S&P?—According to a survey by Synopsys, 36% of the medical device makers, and 45% of the healthcare delivery organizations do not test their medical devices in terms of S&P [14].
2. Is the device known vulnerabilities addressed?—According to a survey by Synopsys, 35% of medical device makers, and 26% of healthcare organizations say that their medical devices contain significant vulnerabilities. 18.3% of device makers and 13% of healthcare organizations say their tested medical device contains malware [14].

4.13 Log Management

This measures the device ability to monitor and analyze all events. For example, this helps the owner of the device to know the users who logged in, to check the data and can find if any unauthorized user or program is able to see or alter the data. A good log management is measured by the following questions:

1. Does the device have a log management system?—Log management system helps the user to know the users who accessed the device and the data.
2. Is the log management system in the device trustworthy?—There are some basic log management systems available which are not reliable.
3. Is the device capable of installing a log management system?—There are different log management systems available which can be easily installed based on the requirement such as Logsign, Splunk, and Log packer.

4.14 Compatibility

This measures the device compatibility with other devices. If the device is compatible with other devices and applications, this means that it can automatically shares the data with those devices and applications. This is measured by the following questions:

1. Is the device compatible with iOS and notifies the user before sharing the data?
2. Is device compatible with macOS and notifies the user before sharing the data?—macOS is an operating system developed and marketed by Apple Inc. It is the primary operating system for Apple's Mac family of computers.
3. Is the device compatible with Android but notifies the user before sharing the data?—Android is a mobile operating system developed by Google, based on a modified version of the Linux kernel and other open-source software.
4. Is the device compatible with Windows but notifies the user before sharing the data?—Microsoft Windows is a group of graphical operating system families, all of which are developed, marketed, and sold by Microsoft.

5 Stakeholder–Centric Approach

The stakeholders for the IoMT wearables include patients, doctor, hospital, nurse, manufacturer, security researcher, and regulatory authorities, insurance. Not all these stakeholders require all the previously defined attributes. Hence, Table 1 depicts the 14 S&P attributes discussed in Sect. 4 as applied to the stakeholder's requirements.

This clearly shows that patients and manufacturers need to consider all the attributes. This is because patients are the main users and their personal data and health data will be stored and communicated from and to the device. Manufacturers also need all attributes to measure S&P in their products and their competitor products.

6 Case Study

In this section, we evaluate the S&P of two IoMT wearables (i.e., Dexcom g5 [15] and MiniMed 530G [16]) using our method. In step 1, we used devices specifications from manufacturer websites to answer the considerations questions for both devices as shown in Table 2. Step 2 of the methodology, the following equation is used to compute the score for each attribute using its considerations. The scores for all the attributes are also normalized to score out of 10.

$$\text{Attribute score} = \sum_{i=1}^{N} \text{Consideration}_i \times \frac{10}{N} \tag{1}$$

All the attribute scores were plotted in a graph for better visualization. Figure 1 shows all the attributes' scores for Dexcom g5 and MiniMed 530G.

Table 1 Wearable IoMT S&P attributes: stakeholder-centric approach

Stakeholders	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Patient	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Hospital		X				X			X					X
Doctor			X	X	X	X	X		X			X		X
Nurse				X		X			X					X
Manufacturer	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Regulatory authorities		X		X							X	X		X
Insurance			X	X	X					X		X		
Security researchers		X	X	X	X	X	X	X			X			X

Table 2 The result of considerations for Dexcom g5 and MiniMed 530G

Attributes	Dexcom g5	MiniMed 530G
1. Authentication and identity management	2.3	5.5
2. Access control and profiling	2.2	2.2
3. Storage location	4.0	4.0
4. Encryption	0.0	0.0
5. Compliance	4.1	3.0
6. Connectivity	2.0	2.2
7. Data shredding	0.0	0.0
8. Classification of data	0.0	6.0
9. Simultaneous data accessed	10.0	10.0
10. Number of stakeholders	10.0	10.0
11. Device bandwidth	0.0	0.0
12. Tested device	4.9	0.0
13. Log management	0.0	0.0
14. Compatibility	0.0	0.0
Total	39.5	42.9

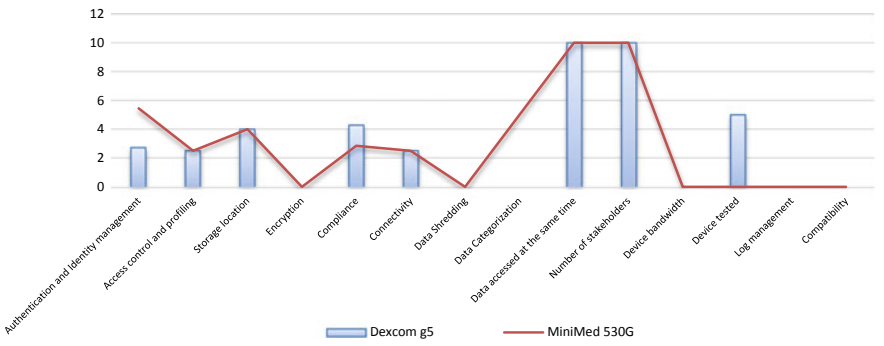

Fig. 1 Comparison of two IoMT wearable devices using the proposed methodology

7 Conclusion and Future Work

Stakeholders of IoMT wearables (i.e., healthcare practitioners and patients) often focus more on the functionality and performance of the device, but overlook the S&P issues associated with these devices. In most cases, the reason to overlook the S&P is lack of proper awareness. Hence, this work presented a methodology to assist IoMT stakeholders to rank IoMT wearables in terms of their protection and deterrence. The novelty of this work lies in that it defines security according to every

stakeholder's interaction with the IoMT wearables. This method aims to assists IoMT stakeholders with different requirements, goals, and tolerance to risks, to be aware of the S&P issues in IoMT and to manage them. It can also help in dealing with stakeholders' conflicts of interests broadly and thoroughly in decision-making.

Our future works include developing a tool with this methodology to easily evaluate the values of any IoMT wearable device. This tool can also be developed to store the values of previously evaluated devices and help the customers to retrieve these values. Finally, for each attribute, weightage can be added as pertinent to the stakeholder.

References

1. Markets, R.: Global wearable medical device market opportunities to 2022. https://www.prnewswire.com/news-releases/global-wearable-medical-device-market-opportunities-to-2022-300542952.html
2. Abie, H., Balasingham, I.: Risk-based adaptive security for smart IoT in eHealth. In: Proceedings of the 7th International Conference on Body Area Networks. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), pp. 269–275 (2012)
3. Savola, R.M., Savolainen, P., Evesti, A., Abie, H., Sihvonen, M.: Risk-driven security metrics development for an e-health IoT application. In: Information Security for South Africa (ISSA), pp. 1–6. IEEE (2015)
4. Alsubaei, F., Abuhussein, A., Shiva, S.: A framework for ranking IoMT solutions based on measuring security and privacy. In: Arai, K., Bhatia, R., Kapoor, S. (eds.) Proceedings of the Future Technologies Conference (FTC) 2018, pp. 205–224. Springer International Publishing, Cham (2019)
5. Food and Drug Administration: Postmarket management of cybersecurity in medical devices. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf (2016)
6. MDRAP | Home Page. https://mdrap.mdiss.org/
7. McMahon, E., Williams, R., El, M., Samtani, S., Patton, M., Chen, H.: Assessing medical device vulnerabilities on the Internet of Things. In: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 176–178. IEEE (2017)
8. Medical equipment in general. https://www.iso.org/ics/11.040.01/x/
9. Laplante, P.A., Kassab, M., Laplante, N.L., Voas, J.M.: Building caring healthcare systems in the Internet of Things. IEEE Syst. J. 1–8 (2017)
10. Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S.: The Internet of Things for health care: a comprehensive survey. IEEE Access. **3**, 678–708 (2015)
11. Williams, P.A., Woodward, A.J.: Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med. Devices Auckl. NZ. **8**, 305–316 (2015)
12. Leister, W., Hamdi, M., Abie, H., Poslad, S.: An evaluation framework for adaptive security for the IoT in ehealth. Int. J. Adv. Secur. **7**(3&4), 93–109 (2014)
13. Recommended bandwidth for health care providers. https://www.greatsys.com/recommended-bandwidth-for-health-care-providers/
14. Medical-device-security-ponemon-synopsys.pdf. www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf
15. zak.huber: Dexcom G5 Mobile CGM System | Glucose on your phone. https://www.dexcom.com/g5-mobile-cgm
16. MiniMed 530G Insulin Pump | Diabetes Pump System With SmartGuard Technology. https://www.medtronicdiabetes.com/products/minimed-530g-diabetes-system-with-enlite