A Reference Architecture Proposal for Secure Data Management in Mobile Health

A Reference Architecture Proposal for Secure Data Management in Mobile Health

1st Mario Angelelli
Dept. of Innovation Engineering
University of Salento
Lecce, Italy
mario.angelelli@unisalento.it

2nd Christian Catalano
Dept. of Innovation Engineering
University of Salento
Lecce, Italy
christian.catalano@unisalento.it

3rd Derek Hill
Panoramic Digital Health
Grenoble, France
derek.hill@panoramicdigitalhealth.com

4th Hristo Koshutanski
Cybersecurity Unit
Atos Research & Innovation
Madrid, Spain
hristo.koshutanski@atos.net

5th Claudio Pascarelli
Dept. of Innovation Engineering
University of Salento
Lecce, Italy
claudio.pascarelli@unisalento.it

6th Joseph Rafferty
School of Computing
Ulster University
Newtownabbey, United Kingdom
j.rafferty@ulster.ac.uk

***Abstract*—Mobile health (mHealth) is becoming a prominent component of healthcare. As the border between wearable consumer devices and medical devices begins to thin, we extend the mHealth definition including sports, lifestyle, and wellbeing apps that may connect to smart bracelets and watches as well as medical device apps running on consumer platforms and dedicated connected medical devices. This trend raises security and privacy concerns, since these technologies collect data ubiquitously and continuously, both on the individual user and on the surroundings. Security issues include lack of authentication and authorization mechanisms, as well as insecure data transmission and storage. Privacy issues include users' lack of control on data flow, poor quality consent management, and limitations on the possibility to remain anonymous. In response to these threats, we propose an advanced reference platform, securing the use of wearables and mobile apps in the mHealth domains through citizens' active protection and information.**

***Index Terms*—mHealth, wearables, privacy, cybersecurity, anonymity**

I. Introduction

Healthy and responsible lifestyles are becoming an important component of modern living. They involve physical exercise, management of stress, maintaining a healthy diet and exercising good sleep hygiene. Mobile Health technologies, such as activity trackers and biometric monitoring, have demonstrated a positive impact on lifestyle and fitness factors [5]. In some cases, these mobile health technologies meet the definition of a medical device [2], either for the entire product, or just for the software running on the consumer hardware platform [3]. The positive impact is leading these technologies into the market of medical devices, where they are used for multiple purposes relating to quantified self, e.g. metric evaluation to assess health intervention and synergetic action with next generation clinical trials of new medicines.

Wearable sensors have the potential to generate big datasets related to physiological factors, due to their variety, integrability, and high sampling rates. Data from these wearables could be aggregated on a global scale and made publicly available for different scopes (e.g. scientific research), using an agreed format for data and knowledge interchange [15], and associated metadata to ensure comparability of data [11]. Wearable generated data also has a sizeable commercial value within many domains. In the example of the insurance domain, such data can inform personalization of insurance premiums which may change as a person's activity levels, and biometric factors, vary [15].

Personal data collected by a wearable device could allow an unsettling insight into the user's health, habits, location and activities. In addition, personal data collected through tracking systems, and wearable devices may include information concerning an individual's health, which are a special category of personal data under the General Data Protection Regulation (GDPR). Health data must comply with a higher level of legal protection, and this is particularly important as stakeholders other than the user, or subscriber, may have access to privacy-sensitive information stored on such equipment. The coexistence of data privacy and limited functionalities deriving from reduced data access and cybersecurity issues is becoming a matter of high priority for medical regulators. The division between personal and non-personal data in such wearable generated datasets is becoming increasingly blurred with technological developments and an increase in the services such devices offer. The unintended consequences of wearable sensors should be considered as such devices, and the data they generate, is not completely secure.

In response to these threats, and given the limitations of already available tools and methods that will be discussed in the following section, the aim of this work is to present an advanced platform for securing, through citizens' active protection, the use of wearables and mobile apps in the mHealth domain. The reference architecture identifies state-of-the-art technologies necessary to implement the platform and scale both the security and privacy needs of stakeholders in the mHealth domain. The platform will help citizens to

better monitor and audit their security, privacy, and personal data protection, enabling them to become more engaged and active in the fight against cyber, privacy, and personal data protection risks.

II. Background Analysis

Networked medical devices, mHealth technologies, and cloud services have the potential to play a transformational role in healthcare, but they may also represent a vehicle to expose patients and healthcare providers to safety and cybersecurity risks. We refer to [10], where one of us and co-authors discuss evaluation and issues of IoT solutions, including data and identity management, for a class of mental disorders. From a sensor perspective, the unintended consequences of wearable sensor use can be summarized by two statements [16]: first, wearable sensors are prone to the (accidental or deliberate) exposure of users' information and privacy; then, there is a high level of trust in sensors and data provided by sensors, therefore they are susceptible to attacks that may potentially harm their users.

Technological weaknesses also rely on low computational power which restricts the complexity of security measures that may be employed, and a high degree of risk associated with updating their firmware, reducing the chance that security flaws will be patched. These vulnerabilities are confirmed by recent research [9]. Common security vulnerabilities that can be exploited in wearable devices are related to the following core factors:

- Lack of authentication and authorization: most wearable devices often do not come with basic security mechanisms such as user authentication, and they typically store data locally without encryption [4].
- Lack of physical security controls: a security vulnerability is the potential for the loss of the device itself [6]. Spying apps can be installed to a smartphone connected to a wearable to identify sensitive typed information, such as a credit card number, based on the wearer's hand movements [12].
- Unsecure local data transmission: wearable devices rely on unsecure local data transmission, such as the widely adopted Bluetooth Low Energy [8]. As a result, an attacker could perform a man in the middle attack [14].
- Data security and privacy in Device-to-Cloud communications: personal sensitive data transmitted from the local storage of the smartphone to the Cloud application may be stolen [arriba2016collection]. Attacks include man-in-the-middle and redirection attacks [6], [7].
- Insecure data storage on the Cloud: data synchronized to a Cloud service could be affected by a number of risks, including implementation weaknesses, distributed denial of service (DDoS) attacks, SQL injection, ransomware, or back door attacks [13].

In addition to the risks related to the security of the network infrastructure and its associated attack surfaces, privacy risks also emerge in the described scenario. Main factors to be considered regarding privacy issues, in line with [17], are the following:

- Lack of control: users may become monitored by third parties, and communication between objects can be triggered automatically, without the individual being aware.
- Quality of the user's consent: users may not be always aware of the data processing carried out by specific objects. Wearable devices may embed sensors that can record and transfer data without individuals' consent.
- Limitations on the possibility to remain anonymous: wearable devices kept in proximity of data subjects result in the availability of a range of other identifiers, such as the unique, openly broadcasted, radio addresses of other devices, which could be useful to create unique fingerprints and stable identifiers attributed to specific individuals.

Currently, available systems are focused on state-of-the-art security issues, but most are not designed to combine active protection from attacks (security) and awareness of personal data flow (privacy) in a manner that may be adapted for a large scale use. Moreover, the majority of these systems are proprietary and closed, therefore posing a threat to users' privacy due to the impossibility of understanding what data is collected and for what purposes. Finally, most of the services and products dealing with security and privacy, often involve little or no interactions with Data Protection Authorities and Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs).

III. Concept and Approach

According to the previous background analysis, the use of mHealth devices and mobile application poses two main challenges, one related to data privacy and one related to data security. With regard to data privacy, it is important to answer citizens about what data is collected, who uses it and for what purposes. In terms of data security, their confidentiality, integrity and availability should be prevented through network anomaly detection that could later pose data at risk.

In the proposed architecture, the citizens' active protection is ensured by a combination of the following items:

a. network monitoring devices able to track incoming and outgoing network traffic generated by mHealth wearables and applications (standalone or paired with the wearables);
b. mobile applications to be installed on the devices that act as gateways between wearables devices and internet with threats detection, dashboarding and autonomous mitigation capabilities;
c. secured-by-design wearable device that connects to a mobile phone or the gateway with threats early detection capabilities.

The provisioning of information to citizens about privacy and security threats related to use of mHealth apps and devices is ensured by:

d. web applications to collect and share information on the reliability (both in terms of privacy and security)

of mHealth devices and applications available on the market;

e. an On-line Chatbot Assistant Service specialized in security and privacy incidents and data breaches notifications;
f. a privacy policy interpretation tool providing user friendly representations of privacy policies for the apps and wearables in the mHealth domain, using alternative media formats.

Where the mobile health technology is a medical device, these collected data could constitute real-world evidence used in the Post Market Clinical Followup Plan of the medical device, as required by the EU Medical Device Regulation [1].

IV. Proposed Architecture

We propose a modular platform for the active protection of citizens' security and privacy, whose constituent modules are described in Section V and can be combined to obtain different configurations applicable in different scenarios. All configurations are based on a subset of a collection of modules that will be described in Section V. The four configurations, of increasing complexity and data security, are proposed below.

A. Basic Configuration

The "basic configuration" provides all these features ensuring an intermediate level of protection for all citizens, providing the installation of mobile applications only. This guarantee, for this configuration, the highest level of acceptability for end users. The basic configuration is presented in Figure 1.

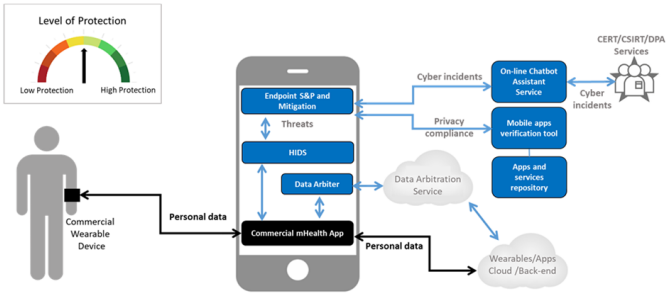

Fig. 1. Basic configuration

B. Intermediate Configuration

The "intermediate configuration" provides greater protection level through the use of an additional device to be installed by the user. This device consists of a Gateway on top of which runs a Network Intrusion Detection System (NIDS) that assists the Host-based Intrusion Detection System (HIDS) to monitor incoming and outgoing network traffic generated by mHealth wearable devices. Due to the dedicated hardware and greater computational power, it is expected the NIDS having greater performance than the HIDS in detecting traffic anomalies. The intermediate configuration requires the user to buy and manage an additional device, but ensures a higher level of protection. This architecture is presented in Figure 2.

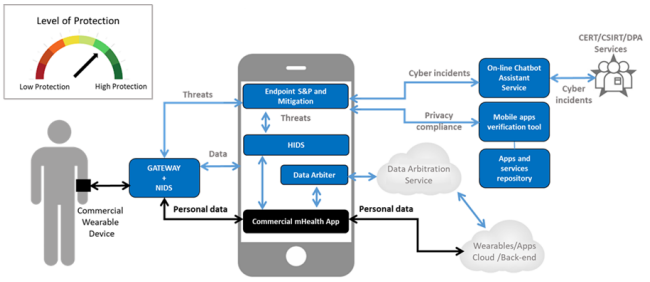

Fig. 2. Intermediate configuration

C. Advanced Configurations

In the basic and intermediate configurations, it has been considered that the citizen uses a commercial wearable device available on the market. This guarantees a high level of acceptability but, consequently, does not ensure the highest level of privacy protection. Commercial devices, which can be considered closed systems, in most cases use proprietary encryption methods. These methods should provide greater accessibility for users, but make the work of NIDS and HIDS systems more difficult, thus making the flow of data opaque to the user.

To overcome this limitation, we propose a last configuration that supports full GDPR compliance and makes use of an open, secured-by-design wearable device specifically designed for a medical purpose, where hardware encryption is provided by the wearable coupled to a gateway. This gateway can be used in both fixed (plugged in at home) and mobile versions. This ensures maximum transparency for the citizen, in terms of privacy, and the highest protection level. This architecture is presented in Figure 3.

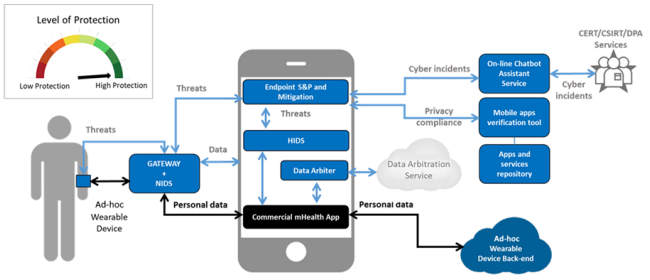

Fig. 3. Advanced configuration.

A variant of the advanced configuration has also been envisaged for situations in which it is desirable to collect wearable sensor data from individuals for medical purposes, without the use of a smartphone. This may arise in medical applications for people unable or unwilling to use a smartphone (e.g. elderly people, people with disabilities, *etc.*), or where a smartphone is found to reduce reliability. In this case, an alternative user interface replaces the smartphone. This architecture is presented in Figure 4.

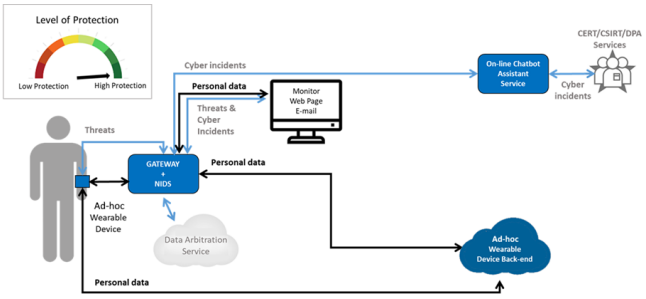

Fig. 4. Variant advanced configuration without smartphone.

V. Modules of the Proposed Platform

Current technology provides a basis to support the feasibility of the architecture proposed in the previous section, as well as its potential implementation. This also comes from the modular approach adopted in the design of the architecture, which can be realized through iterated integrations of services, functionalities, and devices.

Below, we describe eligible tools that can be adopted or developed in order to realize the configurations depicted in Figures 1-4.

A. Gateway & Network Intrusion Detection System (NIDS)

Overview: The device envisages a Network Intrusion Detection System (NIDS) running over a Gateway to monitor incoming and outgoing network traffic generated by mHealth wearable devices. The NIDS consists of sensors to acquire information, a computational engine analyzing the data taken from the sensors, a console to monitor the status of the network (if a smartphone is not available), and a database where a set of rules used to identify security and privacy issues are stored.

Key capabilities: The NIDS is a system that reads (sniffs) traffic passing over the segment of the network where it is located, and it includes network traffic analysis capabilities to identify traffic anomalies. The NIDS allows identifying intrusions, letting users monitor the complete network and verify the compliance with wearables and mobile apps stated privacy policies.

B. Host-based Intrusion Detection System (HIDS)

Overview: The HIDS performs dynamic analysis of the device behavior for detecting suspicious incidents. It is autonomous and runs on the mobile device, without needing connectivity to a remote server for processing activities, thus avoiding the risk of data leakage due to this continuous communication. The HIDS continuously monitors a specific set of features at the device level, without individually inspecting the behavior of each application installed on it, in order to identify the runtime behavior of the mobile device. It can implement detection algorithms for classification (benign vs. malicious behavior). If a suspicious behavior is detected, the HIDS sends a notification to the user.

Key capabilities: The HIDS collects data of the smartphone in real time considering features related to its general behavior, e.g. total CPU usage, memory consumption, battery usage and temperature, total outgoing and incoming network traffic, number of running processes and services, total number of opened TCP sockets, and total number of installed applications. The tool classifies a run time behavior as benign or malicious using dedicated algorithms (e.g. Machine Learning using a training set of benign and malicious behaviors) and estimates the probability of intrusion for a specific acquisition period. The HIDS manages alerts: e.g. if there are three consecutive probable malicious events and if their overall probability of intrusion exceeds a defined threshold, the HIDS sends an alert, e.g. through component F, to the user.

C. Mobile Apps Verification Tool

Overview: The web platform analyzes mobile applications (selected by the user) that are installed or are going to be installed in his device, for security and privacy concerns. The web platform performs both static and dynamic analysis to automatically detect suspicious applications and malicious/anomaly behaviors by executing and monitoring applications in a simulated Android OS environment. The web platform performs:

- Security analysis: it detects and analyzes potential malicious mobile applications for suspicious activities and anomaly behavior. It performs deep malware analysis and security testing.
- Privacy analysis: it checks if the permissions required by a mobile application are: (i) those declared in the manufacturer/developer privacy policies (analyzed and "translated" by means of the Privacy Policy Interpretation Tool); (ii) congruent with the scope/purpose and business scenario of that specific mobile application.

The web platform generates comprehensive and detailed analysis reports with a description of security and privacy risks sharable with CERTs/CSIRTs and Data Protection Authorities.

The results of the analysis are fed into the mHealth applications repository (see point D) and made available to other users that own the same version of the same applications. Most popular mHealth mobile applications, for Android devices, are tested within the project in order to create the core of the mHealth applications repository.

Key capabilities: (i) Perform static analysis: the web platform examines the code of executables to determine control or data flows and certain code patterns of these executables without running them. Static analysis can cover the complete program code because it is not bound to a specific execution of an executable and can give guarantees that apply to all execution of the executable; (ii) Perform dynamic analysis: the web platform monitors the execution of an .apk by inspecting runtime behaviors that correspond to selected test cases. Dynamic analysis can examine the behavior of a suspicious .apk by executing it in a restricted environment and observing its actions. This dynamic technique is immune to code obfuscation attempts to obstruct analysis; (iii) Use an adaptation of

the algorithms of the Privacy Policy Interpretation Tool for analyzing privacy policies; (iv) Generate comprehensive and detailed analysis reports, and the results of the analysis are fed into the mHealth applications repository to be available to other users that own the same version of the same application; (vi) If needed, share the results with CERTs/CSIRTs and Data Protection Authorities.

D. Secure Apps and Services Repository

Overview: A repository where users may search for, find, and retrieve information about mHealth apps and devices that comply with the highest security and privacy standards. The repository includes apps and devices from the market (proprietary and open source) for which a ranking is created according to their degree of security and privacy. Users are also able to pairwise compare apps and devices featured in the repository. The latter uses a continuous feed of analyzed information from the tools developed in the platform to be kept updated.

Key capabilities: (i) Detailed description of security and privacy strengths and limitations of mHealth apps and devices; (ii) Provision of different rankings based on user needs; (iii) Advanced search functionality to serve users' security and privacy needs; (iv) Categorization of apps and devices based on their functionality and security/privacy compliance.

E. On-line Chatbot Assistant Service

Overview: Taking advantage of AI-based solutions, a chatbot assistant specialized in security and privacy incidents and data breaches notifications can be envisaged. It informs and assists citizens in dealing with cyber incidents and reporting those to national authorities such as data protection authorities and CERTs/CSIRTs. The human factor (operator) can be addressed through the help of a highly conversational HMI specialized in contextualizing, categorizing, and structuring cyber incident information to enable citizens dealing with and reporting on such incidents to national authorities through appropriate data format and models. The chatbot assistant offers high-level automation and online availability of a help-desk service seen crucial for timely communication and reporting of cyber incidents.

Key capabilities: (i) Specialized knowledge base of mHealth-related security and privacy incidents and data protection breaches; (ii) Highly conversational-oriented UI specialized in contextualizing, categorizing and structuring cyber incident information; (iii) Integration of data models (including structure and format) of various data protection authorities and CERTs/CSIRTs; (iv) Integration with notification services of data protection authorities and CERTs/CSIRTs through appropriate connectors; (v) Multi-language support.

F. Endpoint Security & Privacy and Mitigation App

Overview: Development of a mobile application providing the main user interface, a mobile dashboard, to any security and privacy incident and data protection breach, and privacy policy visualization. The dashboard integrates visualization of the Privacy Policy Interpretation tool. The dashboard is the direct channel for user situational awareness receiving notifications from: (i) Network Monitoring Device, e.g. network layer anomalies; (ii) Mobile Gateway, e.g. on device pairing or low range communications (Bluetooth/NFC) threats; (iii) Mobile App Verification Tool, e.g. on threats coming from selected Apps installed on the user smartphone; (iv) On-line help-desk service on threats coming from outside that have been found by CERT/CSIRT. The app enables citizens to report any cyber or privacy related incident and data. The reported incidents and data feed the Secure apps and services repository. The application also provides mitigation capabilities user-modulated and consent to actuate and react to anomalies and cyber incidents, such as banning outgoing traffic to anomalous-reported (IP range) destinations to prevent possible privacy leakage or applying encryption (e.g., IBE/ABA) on data communicated to non-trusted cloud servers/back-ends.

Key capabilities: (i) Situational awareness (dashboard) to any security and privacy aspects of wearable devices and mobile applications, including privacy policy interpretation media, and security & privacy threats from network and low-range device communications; (ii) Mitigation capability to detected threats and anomalies with user-in-the-loop modulation on level of mitigation actions applied.

G. Ad-hoc Wearable Device

Overview: As an open architecture, secure wearable device can be a relevant aspect of the platform. We envisage a wearable device designed specifically for a medical purpose and providing capabilities required for full GDPR compliance, including encryption of all sensor derived data at rest and in transit, absence of any personal identifiable data on the device, active threats' detection, and a computational core to enable activity, behavior, and symptom detection in the device using secure configuration.

Key capabilities: The ad-hoc wearable device includes multiple sensors and focuses on providing trustworthy and secure medical data. It could be easily configured for many medical applications, from structured physical activity to more complex behavior detection. The open architecture enables additional behavior and activity detection to be added through an application specific configuration file that contains the machine learning core weights. The device can support BLE transfer of summary data and long-term encrypted raw data storage. Active threat detection (e.g. failed BLE pairings) can be monitored on the device. The wearable can interface with either a smartphone or dedicated gateway (fixed or mobile). The device is a component of the advanced configurations described in Section IV.

H. Privacy Policy Interpretation Tool

Overview: The tool produces user friendly representations of privacy policies for the Apps' and Wearables' in mHealth domain, using alternative media formats to enhance understanding of the privacy policy. Moreover, by providing alternative media format options, people with disabilities can

also select their preferred method of interaction with the privacy policy data, thus making it an inclusive tool. The transformation of privacy policies into media objects can take advantages of semantic analysis in NLP, as well as innovative open-source AI libraries. The analyzed privacy policies can also feed the Mobile App Verification tool, letting it recognize if a mobile app is functioning according to the stated policies.

Key capabilities: (i) Recognition/categorization of privacy policies key items; (ii) Analysis of privacy policy natural language text; (iii) Mapping and transformation of items to suitable media formats; (iv) Indication of missing policy items; (v) User friendly interface and presentation of the transformed policy; (vi) Option to select preferred media type.

I. Right to Erasure, Data Portability, and Distributed Ledger Technology

Overview: Citizens' right of erasure and transfer of their data can be achieved at two levels. The basic and intermediate configurations provide "Level 1" data arbitration functionality, which exists as a mobile application and a backend service. At this level, arbitration services interact with third party services, and the service relies on its security and integrity. The mobile application provides citizens with a number of related controls such as erase, import, and export data. In the advanced configuration, "Level 2" includes and extends Level 1 functionalities by removing the requirement for third party services to operate securely and with integrity. In Level 2, data are stored in a distributed, encrypted, file storage service. The control of encrypted data, as well as their portability, is now enabled by Distributed Ledger Technologies and common data interchange format.

Key capabilities: (i) Production of identities that may be associated with data/data generation; (ii) Mechanisms to enable identity owners (citizens) to anonymously remove their data from third party services or data consumers; (iii) Mechanism and data structures to enable identity owners (citizens) to autonomously transfer data securely between data consumers; (iv) Apparatuses to enable identity owners to manage identities including the ability to transfer, place in escrow and erase them; (v) Functionality to enable citizens to generate and manage an arbitrary number of interlinked identities which are completely disparate when external analysis is applied, protecting side channel leakage of sensitive information/contact.

VI. Conclusion

This work proposes the design of a solution to address the specific needs of end users, healthcare providers, and medical regulators, supporting a modular, integrated platform that empowers individuals' control of the data they generate. Citizens' views of their privacy and security can involve the type of transmitted information, the purpose of information transfer, and details on the subject accessing the information, location, time of access. The balance between such risks and potential rewards is likely to be central to many future commercial, legislative, and regulatory developments in this area.

Future work will be directed towards the development of solutions for the components and to exploit its benefits beyond mHealth, also considering other types of consumer IoT technologies such as those adopted in smart homes. The platform can be adapted to monitor the behavior of such devices and better preserve the security and privacy of users.

References

[1] MDCG 2020-7. Post-market clinical follow-up (pmcf) plan template a guide for manufacturers and notified bodies. https://ec.europa.eu/health/system/files/2020-09/md_mdcg_2020_7_guidance_pmcf_plan_template_en_0.pdf, 2020.

[2] R Beckers, Z Kwade, and F Zanca. The eu medical device regulation: Implications for artificial intelligence-based medical device software in medical physics. *Physica Medica*, 83:1–8, 2021.

[3] Onkar Bedi, Pawan Krishan, and Gaaminepreet Singh. Regulatory requirements for medical devices: an insight. *Applied Clinical Research, Clinical Trials and Regulatory Affairs*, 4(1):16–25, 2017.

[4] Andrea Bianchi and Ian Oakley. Wearable authentication: Trends and opportunities. *it-Information Technology*, 58(5):255–262, 2016.

[5] Jonathan D Browne, David M Boland, Jaxon T Baum, Kayla Ikemiya, Quincy Harris, Marin Phillips, Eric V Neufeld, David Gomez, Phillip Goldman, and Brett A Dolezal. Lifestyle modification using a wearable biometric ring and guided feedback improve sleep and exercise behaviors: A 12-month randomized, placebo-controlled study. *Frontiers in physiology*, page 2094, 2021.

[6] Ke Wan Ching and Manmeet Mahinderjit Singh. Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security & Its Applications*, 8(3):19–30, 2016.

[7] Jiska Classen, Daniel Wegemer, Paul Patras, Tom Spink, and Matthias Hollick. Anatomy of a vulnerable fitness tracking system: Dissecting the fitbit cloud, app, and firmware. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, 2(1):1–24, 2018.

[8] Aveek K Das, Parth H Pathak, Chen-Nee Chuah, and Prasant Mohapatra. Uncovering privacy leakage in ble network traffic of wearable fitness trackers. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, pages 99–104, 2016.

[9] Hossein Fereidooni, Tommaso Frassetto, Markus Miettinen, Ahmad-Reza Sadeghi, and Mauro Conti. Fitness trackers: fit for health but unfit for security and privacy. In *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pages 19–24. IEEE, 2017.

[10] Leonardo J Gutierrez, Kashif Rabbani, Oluwashina Joseph Ajayi, Samson Kahsay Gebresilassie, Joseph Rafferty, Luis A Castro, and Oresti Banos. Internet of things for mental health: open issues in data acquisition, self-organization, service level agreement, and identity management. *International Journal of Environmental Research and Public Health*, 18(3):1327, 2021.

[11] Derek Hill, Diane Stephenson, Jordan Brayanov, Kasper Claes, Reham Badawy, Sakshi Sardar, Katherine Fisher, Susi Lee, Anthony Bannon, Josh Cosman, et al. Metadata standards to support deployment of digital health technologies in clinical trials in parkinson's disease. In *MOVEMENT DISORDERS*, volume 36, pages S561–S561. WILEY 111 RIVER ST, HOBOKEN 07030-5774, NJ USA, 2021.

[12] S. Lurye. Experiment: How easy is it to spy on a smartwatch wearer? https://www.kaspersky.com/blog/smart-watch-research/22536/, 2018.

[13] M. Morgenstern. Product warning! chinese children's watch reveals thousands of children's data. https://www.iot-tests.org/2019/11/product-warning-chinese-childrens-watch-reveals-thousands-of-childrens-data/, 2019.

[14] Nroseth. Data security in a wearables world. http://www.swatsolutions.com/data-security-in-a-wearables-world/, 2015.

[15] SJ Redmond, NH Lovell, GZ Yang, A Horsch, P Lukowicz, L Murrugarra, and M Marschollek. What does big data mean for wearable sensor systems? *Yearbook of medical informatics*, 23(01):135–142, 2014.

[16] Michael Schukat, David McCaldin, Kejia Wang, Guenter Schreier, Nigel H Lovell, Michael Marschollek, and Stephen J Redmond. Unintended consequences of wearable sensor use in healthcare. *Yearbook of medical informatics*, 25(01):73–86, 2016.

[17] WP29. Opinion 8/2014 on the on recent developments on the internet of things. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, 2014.