***International Journal Of Engineering Research And Development***
*e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com*
*Volume 20, Issue 6 (June, 2024), PP. 86-88*

# Development of a Cybersecurity Checklist for a Telemanagement System using Internet of Things (IoT) Technology in Healthcare

Aldo Bernardo Barbosa[1], Vagner Rogério dos Santos[1]
[1]*Department of Ophthalmology and Visual Sciences, Laboratory of Technological Innovations in Health*
*Federal University of São Paulo, São Paulo, SP, BRAZIL*
*Corresponding Author: Aldo Bernardo Barbosa*

***ABSTRACT***
*Every day, there is a significant increase in connected sensors, and in health, it is no different. For this reason, data security has been a major concern in healthcare technologies because hackers or attackers can easily access sensor data and, consequently, important user information. This article aims to present a study in which a checklist will be drawn up to help assess cybersecurity for designing, installing, and auditing Internet of Things (IoT) systems for use in healthcare. It proposes using a list of corrective action points, helping to identify and record corrective actions and thus organizing the solutions that can be used to mitigate possible data security weaknesses. These vulnerabilities were investigated in the three main pillars of data security: Integrity, Confidentiality, and Availability, based on research that cross-referenced information on possible weaknesses from relevant bibliographic references.*

***Keywords:*** *Internet of things; data security; cibersecurity; health.*

---

Date of Submission: 12-06-2024 Date of Acceptance: 25-06-2024

---

## I. INTRODUCTION

The growing range of new technologies incorporated into the healthcare sector must be treated with due attention and seriousness regarding risk management, especially during patient care services provided by the institutions responsible [1], [2].

However, with technological advances, the IoT (Internet of Things) was introduced to the world and has emerged as a great ally for remote hospital equipment management [3].

IoT technologies are already being implemented in various institutions in the healthcare sector, especially in patient care areas. They will revolutionize medicine and people's lives with a proven return on investment in hospitals and laboratories. They will also help to reduce the rate of hospital-acquired infections. Soon, based on information from connected devices, accessing patients' entire histories at any time and from anywhere will be possible [4].

There is a significant increase in connected sensors every day, and healthcare is no different. Data security has been the biggest concern in IoT because hackers or attackers can easily access sensor data. Therefore, it is essential to analyze recent data security methods in IoT [5].

Information security in healthcare is crucial for obtaining quality medical care and market recognition. Technological advances, driven by digital transformation, are also increasing threats to healthcare institutions that must seek cybersecurity services, i.e., advanced security systems that guarantee the protection of patient data [6].

This study aims to develop a checklist to help assess cybersecurity when designing, installing, and auditing IoT systems for use in healthcare.

## II. MATERIAL AND METHODS

The applied research took place at the Laboratory of Technological Innovations in Health (LITS) of the Department of Ophthalmology and Visual Sciences of the Paulista School of Medicine (EPM) - Federal University of São Paulo (Unifesp), based on a bibliographic study of the segment, such as current reading and reference books, periodicals and various publications, from March 2022 to December 2023, without any restriction on date of publication, language and nationality. These studies served as theoretical support for the development of a cybersecurity checklist for IoT systems in the healthcare sector.

To draw up the checklist, cybersecurity weaknesses were cross-referenced from bibliographic references, considering the three main pillars of data security: Integrity, Confidentiality, and Availability [7] – [10].

## III. RESULTS

The checklist presented was organized into specific fields to facilitate evaluation at critical points in an IoT system, thus contributing to the organization of the tasks listed as corrective action points, helping to identify and record solutions that can be used to mitigate possible data security weaknesses.

To identify vulnerabilities in the IoT system, the data security checklist must be applied. This checklist helps identify open doors that make life easier for cybercriminals.

This checklist should be applied at the beginning of the data security analysis, helping to compose the corrective actions and as a validity test at the end once the corrective actions have been applied. It should contain all the information on the person responsible, company, and address, as well as the application area and the auditor and person responsible for the checklist

In the "Status" field, mark Yes or No with an X on the question concerning data security; if the answer is No, a corrective action is generated.

**Table 1: Check List**

| | | | | |
|---|---|---|---|---|
| **Cybersecurity Checklist** | | | | |
| Project: | | | | |
| Technician Responsible: | | | | |
| Initial | Date:____/___/___ | | | |
| Validation | Date:____/___/___ | | | |
| Item | Data Security Questions | Status | | Corrective Action |
| | | Yes | No | |
| 1 | Is the device protected against physical attacks, with no open USB ports and easy access to the microprocessor? | | | |
| 2 | Are passwords for accessing the device composed of at least 12 characters, including numbers, symbols, uppercase and lowercase letters? | | | |
| 3 | Is the communication between the device and the server authenticated? | | | |
| 4 | Is communication between the device and the server encrypted? | | | |
| 5 | Does the communication between the device and the server have a quality of service level? | | | |
| 6 | Does the device receive constant firmware updates? | | | |
| 7 | Is the physical recording environment of the microprocessor firmware controlled? | | | |
| 8 | Is the computer environment for recording the microprocessor firmware access controlled? | | | |
| 9 | Is the computer or firmware recorder disconnected from the internet? | | | |
| 10 | Do employees working with the device receive training on social engineering attacks? | | | |
| 11 | Are the electronic components used to manufacture the device of legitimate origin? | | | |
| | | | | |
| Aproval: | | Review: | | Date: |
| Aproval: | | Review: | | Date: |
| Aproval: | | Review: | | Date: |
| Aproval: | | Review: | | Date: |

## IV. DISCUSSION AND CONCLUSION

It was possible to draw up a checklist to help assess cybersecurity for designing, installing, and auditing IoT systems for use in healthcare. This study has provided important clues and support with theoretical bibliographical references for a deeper understanding of cybersecurity weaknesses in IoT systems used in healthcare. However, future studies must be conducted to apply this checklist in practice to IoT systems in operation to evaluate its applicability and, consequently, its veracity.

## REFERENCES

[1]. Kuwabara, C. C. T., Évora, Y. D. M., and Oliveira, M. M. B. 2010. Risk management in Technovigilance: Construction and validation of a medical-hospital product evaluation instrument. Revista Latino-Americana de Enfermagem, 18:5, 943–951. https://doi.org/10.1590/s0104-11692010000500015

[2]. Lorenzetti, J., Lanzoni, G. M. de M., Assuiti, L. F. C., Pires, D. E. P. and Ramos, F. R. S. 2014. Health management in Brazil: dialogue with public and private managers. Texto & Contexto - Enfermagem, 23:2, 417–425. https://doi.org/10.1590/0104-07072014000290013

[3]. Mishra, P., Puthal, D., Tiwary, M. and Mohanty, S. P. 2019. Software defined IoT systems: Properties, state of the art, and future research. IEEE wireless communications, 26:6, 64–71. https://doi.org/10.1109/mwc.001.1900083

[4]. Paiva, F. (2019 Jan 16). IoT na Saúde: O futuro já começou. Janeiro de 2019. Portal Saúde Business. https://www.saudebusiness.com/ti-e-inovao/iot-na-sade-o-futuro-j-chegou.

[5]. Selvaraj, S. and Sundaravaradhan, S. 2020. Challenges and opportunities in IoT healthcare systems: a systematic review. SN Applied Sciences, 2:139. https://doi.org/10.1007/s42452-019-1925-y

[6]. Almeida, F. and Sauer, J. (9 de abril de 2019). Práticas essenciais para segurança da informação na área da saúde. https://www.pixeon.com/blog/praticas-essenciais-para-seguranca-da-informacao-na-area-da-saude/.

[7]. Kang, K., Pang, Z.-B. and Wang, C. 2013. Security and privacy mechanism for health internet of things. The Journal of China Universities of Posts and Telecommunications, 20, 64–68.

[8]. Gomes, J. T. C. 2019. Riscos e vulnerabilidades dos equipamentos IoT em unidades de saúde. [Tese de Doutorado, Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria].

[9]. Della Rovere, L. and Florian, F. 2022. Estudo sobre segurança e privacidade na internet das coisas (IoT). RECIMA21 - Revista Científica Multidisciplinar, 3:6, e361601. https://doi.org/10.47820/recima21.v3i6.1601

[10]. INTEL. (2022 Apr 15). Segurança de IoT. https://www.intel.com.br/content/www/br/pt/design/technologies-and-topics/iot/security.html/