 doi:10.20944/preprints202007.0369.v1

Article

System for Control and Management of data privacy of patients with COVID-19

Arielle Verri Lucca[1], Rodrigo Luchtenberg[1], Leonardo Garcez[1], Luis Augusto Silva[1,5], Raúl García Ovejero[4], María Navarro-Cáceres [5], Valderi Reis Quietinho Leithardt[1,2,3]*

[1] Laboratory of Embedded and Distribution Systems, University of Vale do Itajaí, Rua Uruguai 458, C.P. 360, 88302-901 Itajaí, Brazil; {...}edu.univali.br
[2] Departamento de Informática, Universidade da Beira Interior, 6200-001 Covilhã, Portugal
[3] COPELABS, Universidade Lusófona de Humanidades e Tecnologias, 1749-024 Lisboa, Portugal
[4] Expert Systems and Applications Lab., E.T.S.I.I of Béjar, University of Salamanca, 37008 Salamanca, Spain.
[5] Expert Systems and Applications Lab., Department of Computer Sciences, University of Salamanca. Pza de los Caídos, s/n. 37007 Salamanca, Spain.
* Correspondence: valderi@univali.br

Abstract: The COVID-19 pandemic plagues the whole world, bringing numerous challenges which need to be addressed. One of them is the privacy of patient data. There are several problems related to data privacy in IoT environments, the use of applications, devices, and functionalities in hospital processes. Therefore, we have compared works from the literature and developed a taxonomy consisting of the requirements necessary to control patient privacy data in a hospital setting in the current pandemic. Based on the studies, an application was modeled and implemented. According to the tests and comparisons drawn between the variables, the application yielded satisfactory results.

1. Introduction

Internet of Things (IoT) devices can be applied in various sectors, acting as a facilitating tool. Devices that help monitor health conditions without the constant need for medical intervention are widely used. There are also wireless technologies that monitor elderly people and remotely send data such as heart rate and blood pressure to their caregivers [1]. In addition to monitoring, there are other devices with auxiliary functions, such as automatic insulin injection devices [2]. These are directly linked to sensitive patient data and provide additional control in critical situations by, for example, setting the dose to be injected into the insulin pump. Both privacy settings and control information must have an extreme level of security. For hospital environments, IoT devices are distributed not only for patient use but also for other functionalities. According to Farahani et al. [3], some of the IoT applications used in hospital settings collect patient data, such as heart rate, blood pressure, or glucose level. As far as the environment is concerned, some sensors detect changes in temperature or control the air conditioning; cameras are used to detect intruders and send alerts. In this context, the scope of the devices ranges from patient monitoring to the evaluation of the environment and the equipment used by health professionals. With their help, the data is recorded from the moment patients are registered at the reception until they are discharged.

When the patient is registered for admission, basic information is collected and complemented after screening. In a first-aid environment, to ensure the safety of all patients, many hospitals use a screening technique known as the Manchester Protocol [4]. After screening, the information is added to the patient's record and the person is given a classification according to their individual condition; this varies from non-urgent cases to cases that require emergency intervention. Sensitive information is added to the user record, whose level of preservation and confidentiality must be treated as critical.

 doi:10.20944/preprints202007.0369.v1

There is information that should not be disclosed or related to the patient, as is the case with a patient suspected of having critical and communicable diseases.

The current pandemic of COVID-19 SARS-CoV-2 (Severe Acute Respiratory Syndrome Coronavirus 2) causes the patient to be identified as a possible carrier even during the screening process, based on certain symptoms. According to Rothan and Siddappa [5], those infected usually show symptoms after approximately five days, the most common signs of illness being fever, cough, and fatigue; the patient may also present headaches, phlegm, hemoptysis, diarrhea, shortness of breath and lymphopenia. These symptoms are identifiable without specific examinations are directly documented in the patient's medical record. Due to COVID-19's high rate of contagion, the patient's referral to medical care and subsequent isolation in the case of confirmation should be done quickly and strictly.

When it is confirmed that the patient has a COVID-19 infection, the information is directly linked to their record, which should remain confidential. Soares and Dall'Agnol [6] comment that privacy is considered an individual right that includes the protection of the intimacy of the subjects, respect for dignity, limitation of access to the body, intimate objects, family and social relationships. And in this same bias, the concern also covers the whole information collected during the patient care process. The application of privacy on patient data must be given to all levels that have access to any information, be it registration, device or image.

For a better understanding of the matter and a clearer overview of the relevant details, this work is organized as follows: chapter 2 lists the related works; chapter 3 describes the taxonomic definition developed for this project and the attributes of the user parameter, environment, privacy, and device; chapter 4.1 demonstrates the modeling of the project, including the use cases, sequence and context diagrams; in chapter 5, we present the prototype with the application developed to be validated. Chapter 6 presents experiments and results. Finally, in chapter 7, we draw the conclusions and discuss future work.

2. Related Work

Studies on the application of privacy in hospital settings cover different aspects. While some address the application of privacy by considering the environment, others consider the device. Different studies were selected to identify the types of privacy targeting, including encryption, profile privacy, device privacy, and taxonomic definitions. Barket et al. [7] present a broad study on the context of privacy, developing a taxonomy meant to connect privacy and technology based on the following aspects: purpose, visibility, and granularity. The purpose, according to the author, is related to the reason that the information is requested; depending on the reason, more or fewer details about the user are passed on. Visibility refers to who is allowed to access the user data. Granularity designates the data transfer required for the type of access and purpose for that particular request. The work of Asaddok et al. [8] involves mobile devices in the area of health (mHealth) and the parameters: usability, security and privacy. The authors propose a taxonomy that involves the three parameters mentioned and, for each, it branches into taxonomies. For usability, effectiveness, efficiency, satisfaction, and learning are defined. For security, confidentiality, integrity, and availability are defined. For privacy, identity, access, and disclosure are defined. The work of Coen-Porisini et al. [9] describes a conceptual model for defining privacy policies that covers the user, the user's profile, the information, and the action that will be taken by a third party to request the information. The authors revealed the link between the three topics mentioned in an UML format. The user is divided into personnel - the person to whom the data is referred; processor – the person who will request the data; controller – the person who controls the actions that can be requested by the processor. Data is divided into: identifiable – in situations when it is clear who the data refers to, such as the name; sensitive - refers to information, processing, and purpose.

Figure 1 shows the sequence described by the authors. We can observe that there is an interaction between the medical user and the controller, along with the processes of access (processing), treatment

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

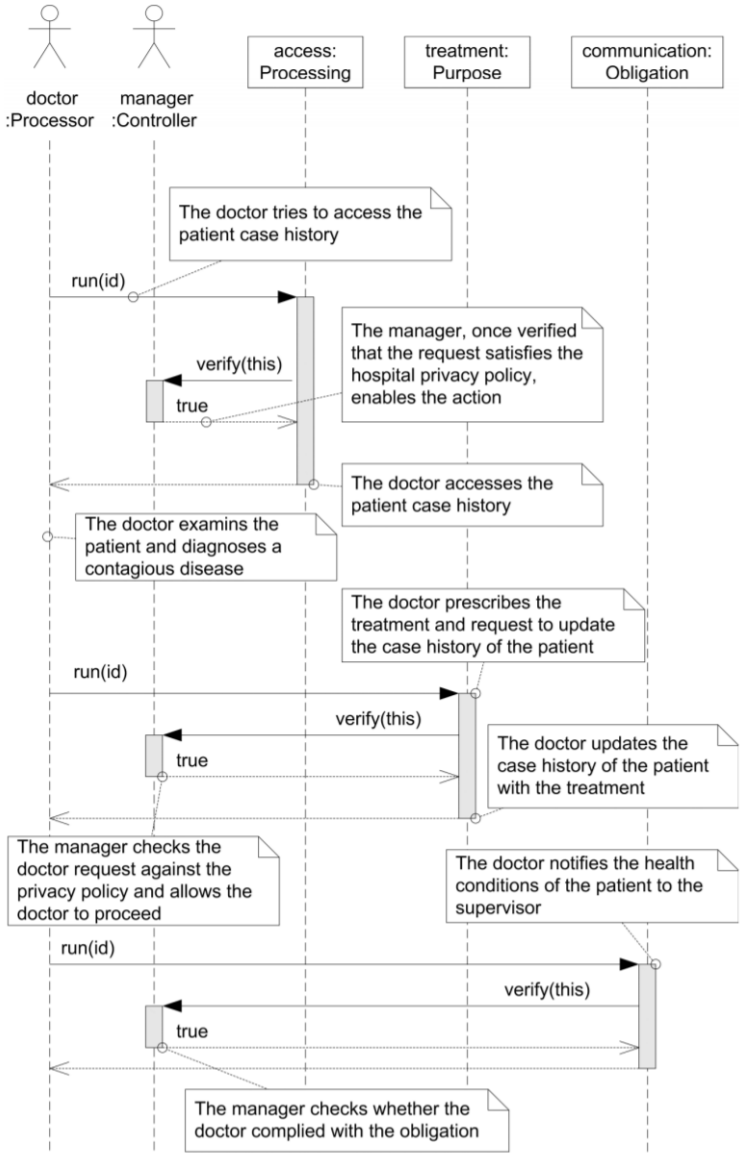

Figure 1. The sequence diagram in the hospital environment [9]

(purpose), and communication (obligation). The diagram demonstrates how information is delivered to the medical user through requests, based on their access profile.

In this context, Silva et al. [10] use a notification management system focused on user privacy. It contributed to the development of an application that can handle different types of notifications. Besides, the system made it possible for those involved to make sure that the messages sent and/or received followed the rules defined earlier. If applied to health notifications or to alert cases of COVID-19, this is an important tool. Addressing notifications with defined priorities, while also linking privacy in the traffic sent. Therefore, this work contributes to finding a link between IoT requirements and definitions.

In [11], the authors implemented a system for monitoring and profiling based on data privacy in IoT. From the results obtained in the tests, they identified different profiles assigned to random situations. In this case, profile priorities for the health system user would apply and identify which profiles would be authorized to receive data. In this work, it was also possible to address the evolution and reduction of the hierarchy based on factors that identify the frequency of users in the environments tested.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

Concerning the relationship between data privacy and its use in situations such as the COVID-19 crisis, the work of [12] deals with the basic concept of human rights that relates data privacy with the need to use certain information, such as someone's location. The authors mention features of applications developed by China, South Korea, and the United States that use tracking techniques to indicate close contact with virus carriers or to identify the movements of certain individuals or groups. The study concludes that the use of location data is important in the fight against the spread of the virus, but that there is other relevant information, such as genetic data, which should be considered as well. It is necessary to use this information correctly, as stipulated by the law. It also states that data sensitivity classification is contextual; data protection and privacy are important and must be maintained even in times of crisis; information leaks are inevitable, so organizations should always protect themselves; ethics in data manipulation is mandatory for more efficient analysis. The work of [13] deals with the privacy of patients' data in terms of the interoperability of systems and the employees' access to information. In addition, it tells us that there is no framework for evaluating privacy audit tools in hospitals yet. The application of a framework for this precise purpose would help to identify any trend in accessing the data and allow the hospital to improve its performance in detecting possible data leaks. According to the authors, the literature reveals that the greatest leakage of information occurs through employees (nurses, doctors, sellers, and others). An evaluation framework was then developed and tested using the concept of the black box, which uses information for usability testing. The following must be monitored through machine learning or artificial intelligence tools: employee access to information; validation of access and non-standard behavior; monitoring of unexplained access to files.

The work of Islam et al. [14] deals with a survey on the application of IoT devices in the health system. The authors deal with the topology of the IoT network for health, which facilitates the transmission and reception of medical data and enables the transmission of data on demand. They also mention features of wearable devices, which capture and store patient data. These may include blood sugar levels, cardiac monitoring, body temperature and oxygen saturation, among others. The authors explain that the security requirements applied to healthcare IoT equipment are similar to those of other communication scenarios. Therefore, the following must be considered: confidentiality, integrity, authentication, availability, data update, non-denial, authorization, resilience, fault tolerance, fault recovery. Figure 2 displays the security issues of IoT devices in the health area.

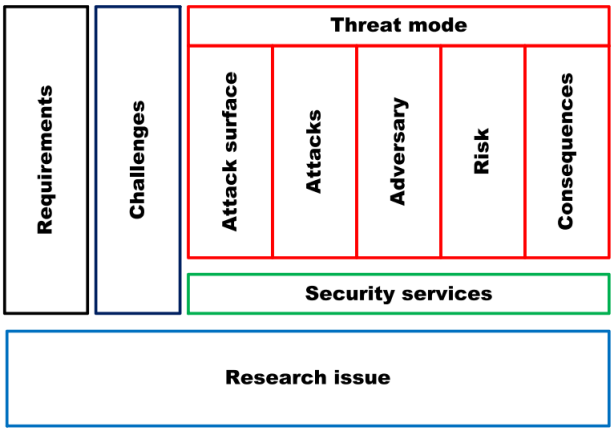

Figure 2. Security issues in IoT-based health care. [14]

Sun et al. [15] designed the HCPP (Healthcare System for Patient Privacy) system to protect privacy and enable patient care in emergency cases. The entities defined for the system are the patient, the doctor, the data server, the family, the personal device, and the authentication server. According to the authors, the system meets the following security criteria: privacy, data preservation by backup, access control, accountability, data integrity, confidentiality, and availability. Figure 3 shows the architecture of the system proposed by the authors.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

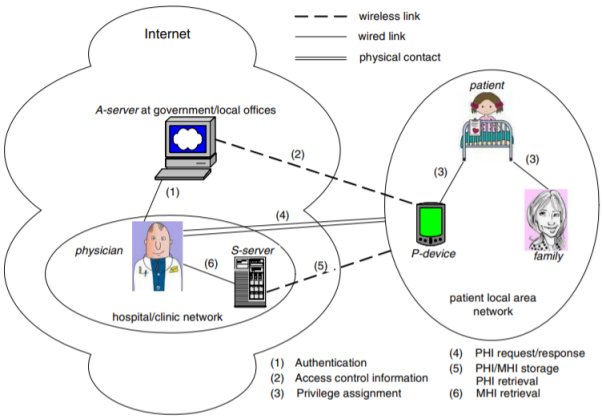

Figure 3. The architecture of HCPP. [15]

Samaila et al. [16] developed a survey in which information was collected regarding work on security and privacy in IoT in general. The scope of the survey ranges from security, encryption, communication protocols, authentication to privacy, among others. The authors also collected information on applications, reliability, and other technical issues, combining 10 related works. Additionally, the authors claim that the work covers a system model, a threat model, protocols and technologies, and security requirements. The work discusses the IoT architecture considering nine application domains: home automation, energy, developed urban areas, transport, health, manufacturing, supply chain, wearables, and agriculture. Security measures and system and threat models were defined for each of the application domains, including protocols and communications. The security properties covered were confidentiality, integrity, availability, authenticity, authorization, non-repudiation, accountability, reliability, privacy, and physical security. These also describe mechanisms that can be applied to achieve the desired security requirements, namely, authentication, access control, encryption, secure boot, security updates, backup, physical security of the environment, device tampering detection.

The related works we have selected cover the topics that we cited as important to privacy. Data encryption is necessary so that, in the event of an attack, a third party cannot gain access to information [17]. The user's profile privacy serves to protect any information from being used by third parties [18]. At the device level, a security layer should be applied to prevent third parties from accessing information or even gaining control of it [19]. Table 1 presents a comparison with the related works concerning the application of the privacy aspects described above with the additional taxonomy application.

The encryption application meant to protect the data was found in the works of[14], [15] and [13]. The related works did not contain any direct mention of it; instead, it was briefly cited in [13]. The privacy application in the user profile is cited by all related works. The creation of a taxonomy was proposed in the works of [7] and [8]. In comparison to the selected works, ours stands out because it includes both the indication of encryption and profile privacy and the definition of the taxonomy meant to define the theme and scenario of the application more clearly.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

Table 1. Scope of related works

Work	Cryptography	Private Profile	Devices	Taxonomy
[9] (2007)		•		
[7] (2009)		•		•
[14] (2015)	•	•	•	
[15] (2015)	•	•	•	
[8] (2017)		•	•	•
[10] (2019)		•	•	•
[11] (2020)		•	•	•
[12] (2020)		•	•	
[13] (2020)	•	•	•	
Proposal	•	•	•	•

This work also contributes to the development of an application with data privacy definitions, parameters, and criteria focusing on records of patients infected with COVID-19. Therefore, we consider that the possibility of contagion can be identified in the first moments spent in the emergency room by means of basic information on the health status together with the monitoring of the feverish state with the use of IoT devices. The degree of privacy applied in the registration process of each user should enable the identification of infected patients without the exposure of sensitive data. To this end, we have developed a taxonomy that highlights how important it is for confidential information to be handled with care. We have included examples of privacy applications in the use of IoT devices for the purpose of receiving, screening, and providing patient care with a focus on the COVID-19 pandemic.

3. Taxonomy

For a better classification of the items related to the privacy parameters used, we have developed a taxonomic definition. This definition covers four parameters for managing privacy standards in hospital settings within the previously defined context. The selected parameters were considered necessary for this scenario. Each parameter consists of five attributes. Figure 4 shows the taxonomic definitions proposed in this project.

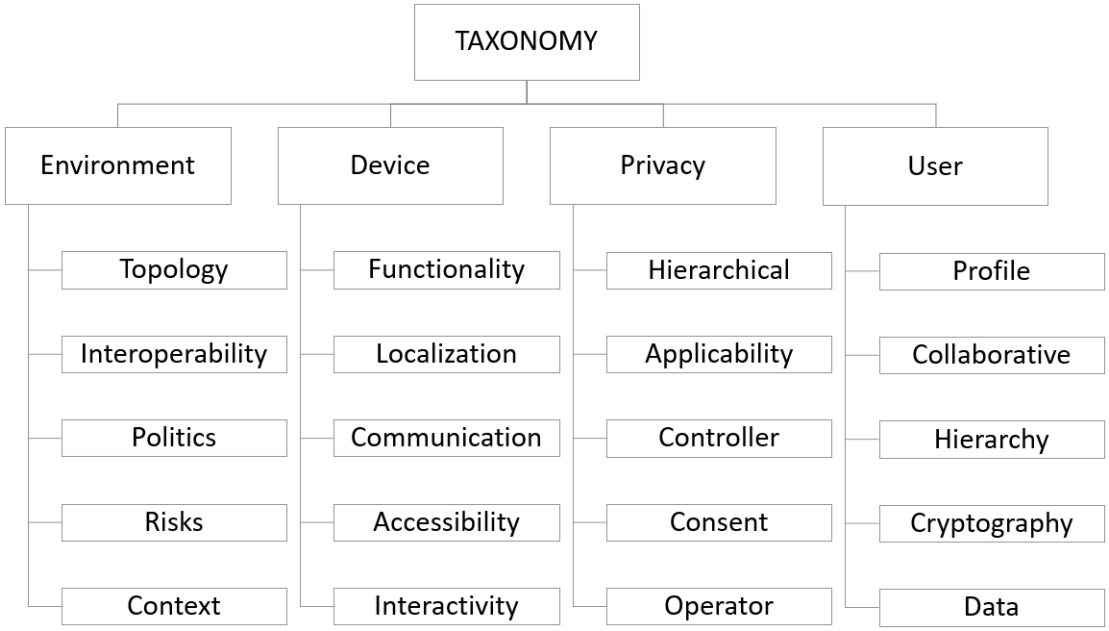

Figure 4. Taxonomia

 doi:10.20944/preprints202007.0369.v1

3.1. User Parameter

The user parameter designates the person that provides, controls, or operates the sensitive data which will be used in privacy handling. This parameter refers not only to the patient but also to anyone who participates in the provision or control of the data. For this parameter, we set the following attributes: profile, collaborative, hierarchy, encryption, data. The profile attribute covers several items that will be part of the process. According to Fengou et al. [20], six entities participate in interactions taking place in the hospital environment: the patient himself/herself; the clinical network that will care for the patient, including doctors, family members, volunteers, health insurance provider, inter alia; the hospital; smart home as an environment with ubiquitous equipment capable of providing security and quality of life; the environment in which the patient works, the vehicle with which the patient is transferred to the clinical center. Based on the entities listed, it can be observed that the user profile is one that must be substantiated, along with the profiles of other entities. The patient's cooperativeness in providing their registration data is fundamental for a better experience in the given setting. According to Leithardt [21], the user must provide access to their information and services, thus favoring both their experience in using the service and the improvement of the system as a whole. The hierarchy enables proper separation of the levels and permissions of each user type. Viswanatham and Senthilkumar [22] proposed the so-called hierarchy-based user privacy, where the information is encrypted and decrypted based on access levels and releases.

The General Data Protection Regulation (GDPR) deals with the need to protect confidential data and the inevitable risk of data theft. Encryption reinforces that all sensitive information must be protected by an acceptable level of security, either at its source or at its destination. According to [23], patient confidentiality is one of the major obstacles in obtaining medical data, as some information is not shared for fear of it being saved in databases that do not comply with security regulations. The protection of sensitive patient information is an essential task. The HIPAA Privacy Standard (Department of Health and Human Services, 2002) [24] deals with the protection of sensitive patient information in the medical field. It is a US federal law created in 1996 to impose standards for the protection of such information and prevent it from being shared without the patient's consent. cooper2005managing deals with privacy and security in data mining in the medical field and cites HIPPA in matters related to information privacy. Written in 2002, it suggests that protective measures be imposed by health plans, clinical centers, and other entities involved.

3.2. Environment Parameter

The environment parameter represents the smart physical location where user data will flow between different systems and devices. For this parameter, we define the following attributes: topology, interoperability, policies, risks, hierarchy. Topology refers to the architecture of a hospital environment. [25] comments that hospitals used to be built with an emphasis on the utility of the building and the technique used. The processes and dynamics of the health field are often determined by how the wards, sectors, and departments that house distinct processes are arranged. In many of the processes that take place during the patient's journey through the emergency room, one or more systems are used.

Interoperability between systems is strongly present in the medical field nowadays. According to Lopes [26], systems used to be designed and developed from an internal perspective of organizations, with no motivation for integration with other systems. In all of the smart environments that people transit, data is shared between information systems and IoT devices. According to Poleto et al. [27], data are a vital part of the operation of a health institution. To apply access security to these environments and define what data will be exchanged between systems and devices, several policies need to be established. According to [28], information security management is an activity that aims to implement a set of policies that help to define an acceptable level of security in these environments, minimizing the potential risks inherent in the exploitation of this information.

 doi:10.20944/preprints202007.0369.v1

Risk management in hospital settings is a crucial activity for the proper functioning of the operation. According to [29], the risk is an estimated value that takes into account the probability of occurrence of damage and the severity of said damage. Therefore, procedures meant to minimize those factors need to be mapped, controlled, and defined. The dimension in the patient's care is large and complex. It occurs at various times and in various environments in the course of service, along with several interactions between the patient, other participants and technologies. [6] emphasizes that, due to its characteristics and complexity, the hospital environment favors the establishment of power and asymmetrical relationships between the nursing team and patients. The asymmetry results from the patients' fragility and vulnerability in the face of health-diseases processes.

3.3. Privacy Parameter

The privacy parameter designates the way in which each piece of information will be handled, according to its characteristics. For this parameter, we define the following attributes: communication, applicability, controller, consent, operator. The communication is linked to the type of user profile, and will usually involve unsafe means of transmitting the information. According to Machado [30], anonymization or encryption in particular pass through the means of communication. That is, the very existence of communication drives the need to apply security measures to data. It is a basic human right to have one's sensitive data handled with care. Thus, its applicability is extremely important. The LGPD - General Data Protection Law [31] aims to apply standards and laws that regulate and protect the data of individuals. Without this application of standards and regulations, sensitive information could easily be used by those who should not have access to it in the first place.

There is a categorization that determines who has the authority to make decisions regarding the type of treatment that personal data will be submitted to. As mentioned in the LGPD [31], the controller has to obtain the consent of the individual owner or holder of the concerned data. The user may, in turn, deny or grant access to their information by a third party. To provide personal data, the user must give their consent, a manifestation by which they agree that their information be used in a specific way for a specific purpose. As mentioned in the LGPD [31], if the controller wishes to use this data at another time, regardless of the purpose, consent will be requested once more. The operator shall be responsible for carrying out the data processing determined by the controller. As mentioned in the LGPD [31], the operator is jointly and severally liable for the damages caused by data handling if the strategy does not comply with legal provisions or is not in line with the controller's instructions. The user provides their consent and the operator is responsible for processing the information made available when for personal use or transfer to third parties.

3.4. Device

The device represents the IoT equipment that will be present in the smart environment and that will interact with the patient's data. For this parameter, we define the following attributes: function, location, communication, accessibility, interactivity. The device must meet the needs of the function to which it will be directed. According to Lupiana and O'Driscolle Mtenzi [32], one of the relevant requirements for devices is their storage and processing capacity. The location attribute refers to the location where the device is installed. For Leithardt [11], the attribute that controls location must be linked to a database where all user data must be included. This database will be accessible only for updating and validating some data. The other information should be processed from the point where the user has accessed the system in order to provide greater security and reliability.

The way the device communicates with the user is addressed by means of the communication attribute and fits in heterogeneity, a feature that ensures information is handled evenly. According to a study presented by Pradilla, Esteve, and Palau [33], the devices are responsible for handling data acquisition through sensors, supporting data treatment with processing units, and acting in conjunction with IoT. Therefore, it is necessary to use heterogeneity both in the communication protocols that are handled by the device and in the number of services and types available. This attribute is associated

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

with the protocols of the device, providing security in data transfer. The possibility to access the device whenever necessary is crucial, and interactivity between the device and the client must be ensured. With this in mind, we have developed a model based on the characteristics and functionalities defined in the described taxonomy.

4. Project Modeling

The model consists of use case diagrams, sequence diagrams, and context diagrams. All of these notations are based on UML (Unified Modeling Language).

4.1. Use Cases Diagrams

The first use case, shown in Figure 5, represents the entry of a patient into the emergency room. The patient interacts with the receptionist and performs some procedures. This use case includes some of the attributes of the proposed taxonomic definition: privacy, represented by the data which the patient grants access to and is registered in the systems; user, represented by the patient and the receptionist; environment, represented by the emergency room.

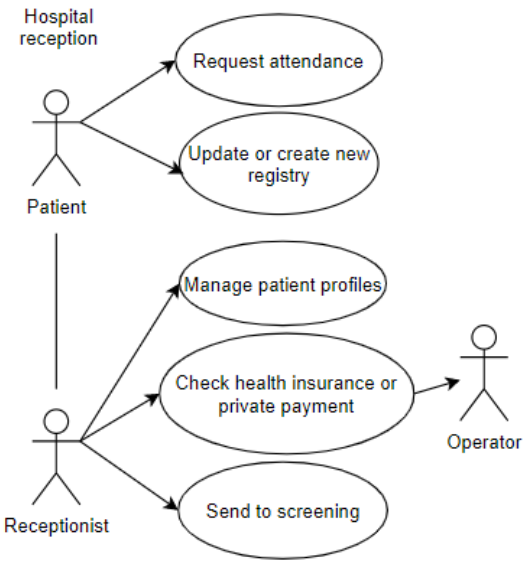

Figure 5. Use Case - Reception at the Emergency Room

The transfer of the patient to the screening area, after first care and registration, is demonstrated in the use case pictured in Figure 6. The screening process aims to establish the urgency of the case and the risk classification. This use case includes some of the attributes present in the proposed taxonomic definition: privacy, represented by the data which the patient grants access to and is registered in the systems and the device; user, represented by the patient and the nurse; environment, represented by the screening room; device, represented by the wearable IoT device that will receive an identification to record the data and the classification of this patient.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

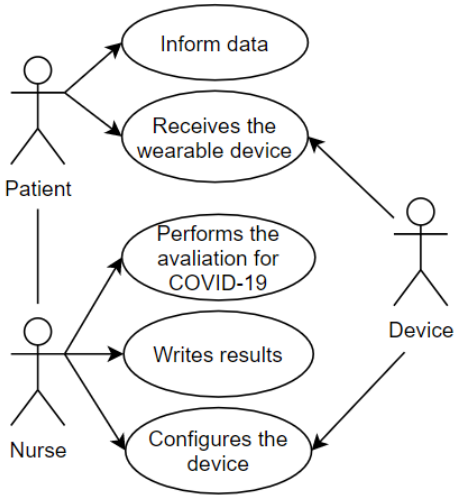

Figure 6. Use Case – Screening Room

The use case illustrated in Figure 7 represents the patient being attended to by the doctor in the office, after going through the screening process. The device identifies the patient so that the data is made available and the doctor proceeds with the consultation. The doctor performs the anamnesis and records the data in the Electronic Health Record (EHR). This use case uses some of the attributes of our taxonomy as follows: privacy, represented by the data which the patient grants access to and is registered in the systems; user, represented by the patient and the doctor; environment, represented by the office; device, represented by the *wearable* IoT device used by the patient.

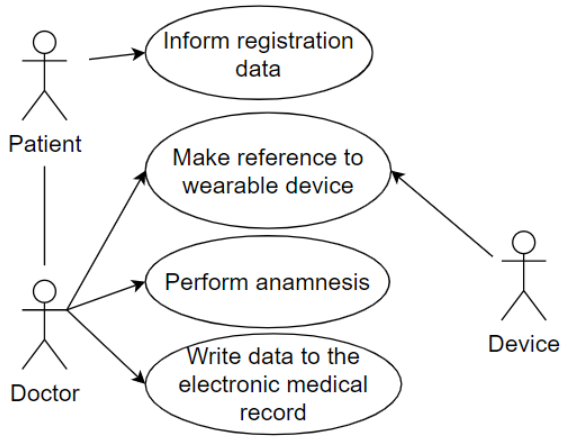

Figure 7. Use Case – Reception at the Office

Sequence diagrams of each use case were also developed. Sequence Diagram is a UML tool used to represent interactions between objects in a scenario, performed through operations or methods (procedures or functions) [34].

4.2. Sequence Diagrams

The sequence diagram displayed in Figure 8 represents the entry of a patient into the emergency room. It demonstrates the arrival of the patient (user) to the emergency room (environment), where they request assistance from the receptionist (user). The receptionist provides a password to the patient waiting to be called on. Upon being called on, the patient provides data for registration updates (privacy), which is recorded by the receptionist in the hospital system. The receptionist checks if the patient has a health plan and then records how the billing issue for this service will be managed. After this procedure, the patient will be referred to screening.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

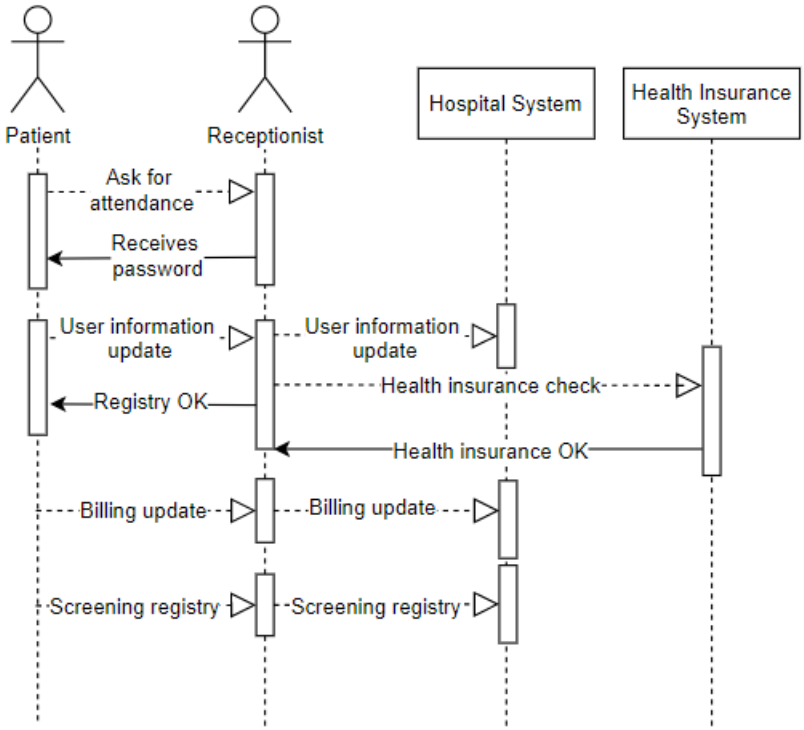

Figure 8. Sequence - Reception at the Emergency Room

The sequence diagram displayed in Figure 9 represents the patient's entry into the screening room after having completed the first stage in the emergency room. It represents the arrival of the patient (user) to the screening room (environment), where they will convey their data as requested by the nurse (user). The nurse records the data in the hospital system and the entry into the system that generates the device (device). The receptionist then hands the device over to the patient and starts the assessment. The patient answers the questions (privacy) and the nurse records all the information in the hospital system. At this time, all patient data is in the system and it can be tracked by the hospital from their wearable device.

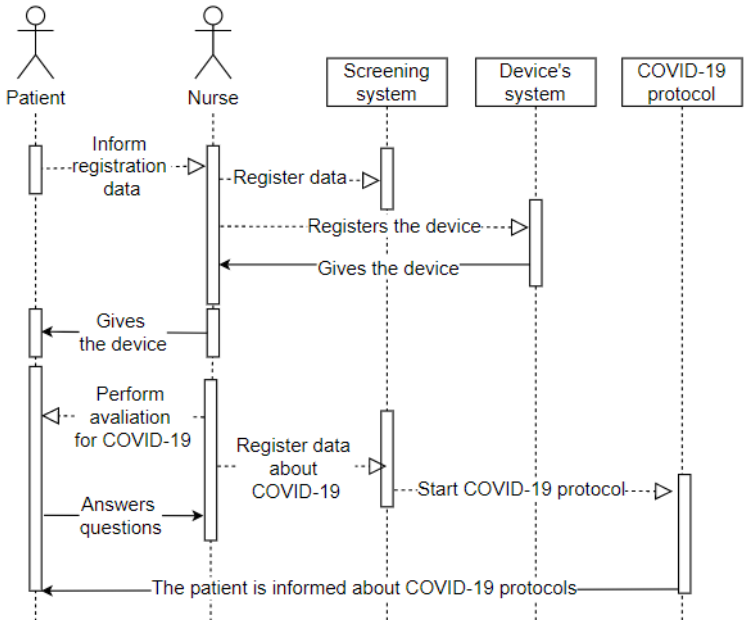

Figure 9. Sequence – Screening Room

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

The sequence diagram displayed in Figure 10 shows the patient's entry into the office after going through the screening process. It represents the arrival of the patient (user) to the office (environment), where they will convey their identification data as requested by the doctor (user). The latter records the data in the electronic record and refers the patient's device (device) in the hospital system. The doctor performs the anamnesis on the patient, who must answer the questions (privacy). The doctor also records this information in the patient's electronic record. From this point on, the patient has already been attended to, so they are medicated and released or referred to another hospital ward due to the evolution of their clinical condition.

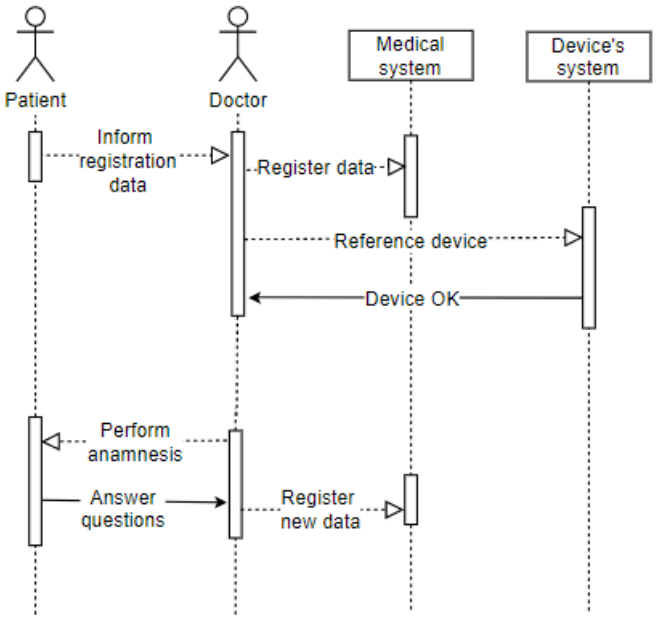

Figure 10. Sequence – Office

4.3. Context Diagrams

The Context Diagram is a UML tool that represents the entire system as a single process. It consists of data streams that show the interfaces between the system and external entities [34]. The diagram is a way of representing the object of the study, the project, and its relationship to the environment.

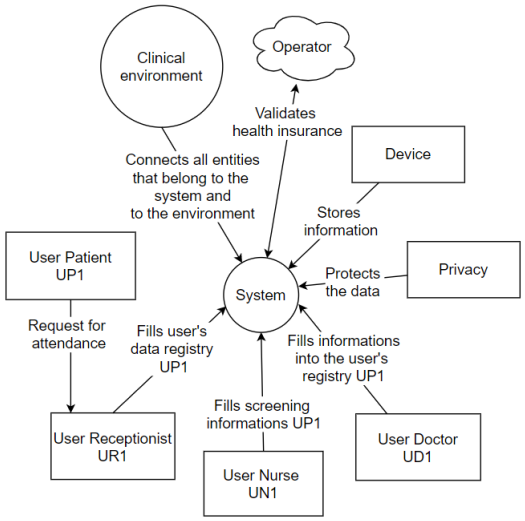

Figure 11. Context Diagram

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

Figure 11 represents the context diagram of this project. The patient (user) requests assistance from the receptionist (user), who will fill in the data (privacy) in the hospital system. The hospital system interacts with the operator's system that is outside the physical environment of the hospital. In the screening process, the nurse (user) conducts the questionnaire with the patient (user), entering the basic health data in the central hospital system, which in turn interacts with the device system. Finally, the doctor (user) performs the anamnesis, entering the consultation information in the central hospital system. These information registration processes are focused on privacy determinations, and all processes take place in a clinical setting, represented specifically within the context diagram.

5. Prototype

A mobile application was developed as a prototype to illustrate the basic principles of a system, from the admission of the patient to the emergency room and referral to the office or discharge indication. The application was developed using Node.Js and was written in Java.

The application is comprised of an initial customer registration screen, which simulates the process of filling out the registration form upon admission to the emergency room. The prototype only contains the basic fields: name, gender, age, CPF, and address. The 'encrypt data?' checkbox has been included so that the encryption/hash algorithm can be selected. Since it is merely a prototype for demonstrating the flow of information and its security application, the hashes SHA-256 and SHA-512 were made available - in the real application, they wouldn't serve to encrypt data because hashes are not reversible and are considered a one-way function [35]; the prototype also includes the AES symmetric encryption algorithm. Figure 12 illustrates the first registration screen of the application with the fields mentioned above.

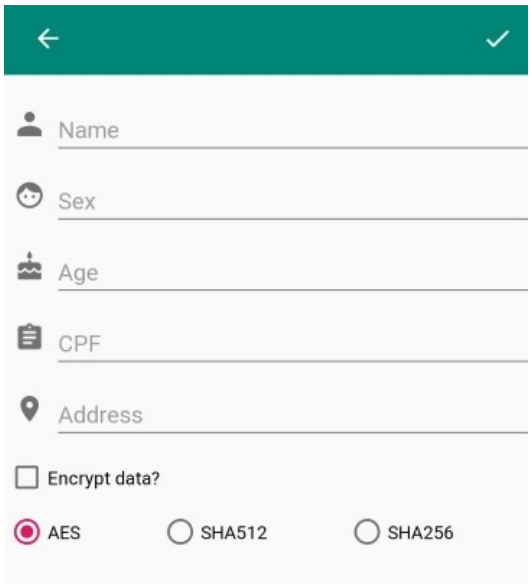

Figure 12. Data entry screen on the mobile app

The flow of the application is as follows: initially, the patient fills out a form with personal data and then is sent to the screening room to answer more questions and thus help medical personnel assess their situation. All the information collected about the patient and their health status is included in their digital record. If communication with other systems is required, the information to be sent is encrypted.

The integration of a *wearable* device for capturing health data, such as temperature and vital signs, is planned. The link between this device and the patient's file allows the information to be collected without the intervention of a health professional. Based on the information provided by the *wearable*, the system makes a temperature analysis. If the patient remains in a feverish state, they are referred

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

to the doctor's office. Since fever is one of the symptoms that prevail in the detection of COVID-19, its absence can prompt a discharge. However, the absence of fever is not a guarantee that there is no infection with the virus [36], so careful monitoring is needed. In addition to the factors described, comparative tests were performed to validate the application based on the requirements that were initially defined in the taxonomy.

5.1. Pseudocode

The algorithms applied in the development of the prototype application are described below in pseudocode format. Pseudocodes cover the generation of a service number, temperature monitoring, and referral in case of emergency.

Pseudocode 3 deals with the generation of the service number, where the patient's data will be saved in an encrypted form and forwarded to the monitoring room. In the monitoring room, the service number to be linked to the customer will be generated.

Input: REST POST request packet
Output: Attendance number
save encrypted packet data
send to monitoring room
return attendanceNumber

Pseudocode 2 deals with the process of monitoring the patient's temperature. The temperature is collected during the period defined by the medical team and, if it is higher than 38.5°C, the patient is referred to the ICU; if it is equal to or above 37°C for five minutes, the patient is referred to another ward for medical assistance; if it is less than 37°C for ten minutes, the patient can be released.

Input: REST POST request packet
Output: Forwarding
while *not forwarded* **do-** **1**
if *temperature* > *38.5* ^{o}C **then** − **2**
$forwardtotheintensivecareunit$
$temperature >= 37 for 5 minutes$
$forwardtothedoctor$
$temperature < 37 for 10 minutes$
$forwardbacktohome$

Pseudocode 2 deals with the alert generated for the ICU in cases where the patient is classified as an emergency. If there is no emergency, the alert is generated for the doctor, informing that the patient will be referred for care.

Input: REST POST request packet
Output: Attendance number
when patient need
if *has urgence* **then-**

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

page the intensive care unit
else
    page doctor
end if

Testing pseudocodigo lib

Algorithm 1: GET_to_Full_Read_request

Input : REST POST request packet
Output: Attendance number

```
1 if has urgence then
2     page the intensive care unit
3 end if
4 else
5     page doctor
6 end if
```

6. Tests and Results

The flow of controlled information in the application starts after the registration data has been filled in; it is also possible to apply other requirements such as a type of encryption to the patient's data. The information in the patient record is integrated with the information provided by the wearable device. Figure 13 illustrates the integration of basic patient information and also reports that the patient was sent for temperature control. The temperature was captured by the device and sent to the system, which in turn will classify the feverish state, suggesting different referrals for each scenario. If the patient exhibits a feverish state and has other symptoms that may characterize COVID-19, their care must be provided in a differentiated way.

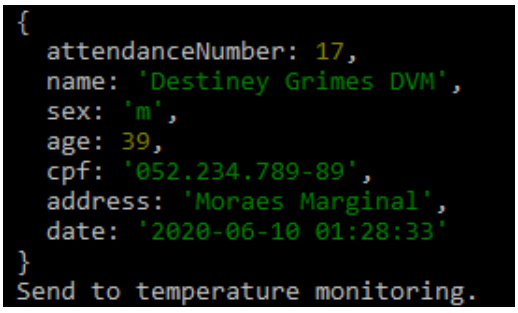

Figure 13. Saved Information

When choosing the type of encryption in the data registration process, the level of data security increases, and the information should only be made available to those who have permission. For prototype demonstration purposes we use the AES symmetric key encryption method. The encryption application aims to secure data while transferring it to other devices. Figure 14 shows the encrypted patient registration data.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1


```
{
  "name":"46070d4bf934fb0d4b06d9e2c46e346944e322444900a435d7d9a95e6d7435f5",
  "cpf":"efa45c803061f485ad7a297d26253fef7764d1891e88dc8be4574d4d89f30cb2",
  "date":"2020-04-05 01:31:12",
  "address":"46070d4bf934fb0d4b06d9e2c46e346944e322444900a435d7d9a95e6d7435f5",
  "age":"c2356069e9d1e79ca924378153cfbbfb4d4416b1f99d41a2940bfdb66c5319db",
  "sex":"46070d4bf934fb0d4b06d9e2c46e346944e322444900a435d7d9a95e6d7435f5",
  "encripted":true
}
```


Figure 14. AES Encryption

After the patient has been registered and the information is stored safely, the data is sent to a system that constantly gets updates on body temperature. With the application of this prototype, we also tested the hypothesis that an IoT device can monitor the patient for changes in temperature. To test the hypothesis, we implemented a set of random values that were read by the program to simulate this monitoring process. Every minutes, the device will check the temperature of the patients who have entered the system and are waiting at the reception of the emergency room. If their temperature can be characterized as feverish, then they are taken to the office with priority. Figure 15 describes the monitoring of a patient whose temperature remains stable and hospital discharge is suggested.

```
Attendance number: 84. Patient Name: Demarcus Kris. Temperature: 38.20. Date:
Attendance number: 85. Patient Name: Phoebe Buckridge. Temperature: 38.85. Dat
Attendance number: 85 foward to the intensive care unit.
2020-06-10 05:10:10 28 entries.
Attendance number: 82. Patient Name: Estell Walter. Temperature: 36.16. Date:
Attendance number: 83. Patient Name: Estella Kutch. Temperature: 37.92. Date:
Attendance number: 84. Patient Name: Demarcus Kris. Temperature: 37.29. Date:
Attendance number: 85. Patient Name: Phoebe Buckridge. Temperature: 38.34. Dat
Attendance number: 86. Patient Name: Bernie Pollich. Temperature: 36.84. Date:
Attendance number: 87. Patient Name: Enos Yundt. Temperature: 38.04. Date: 202
Attendance number: 88. Patient Name: Lambert Yundt. Temperature: 37.49. Date:
Attendance number: 89. Patient Name: Aimee Botsford. Temperature: 37.80. Date:
Attendance number: 90. Patient Name: Brant Denesik. Temperature: 37.27. Date:
Attendance number: 91. Patient Name: Eula Beahan. Temperature: 37.49. Date: 20
Attendance number: 92. Patient Name: Ms. Bernardo Funk. Temperature: 38.49. Da
Attendance number: 93. Patient Name: Buford Hilpert. Temperature: 39.73. Date:
Attendance number: 93 foward to the intensive care unit.
2020-06-10 05:10:30 27 entries.
Attendance number: 83. Patient Name: Estella Kutch. Temperature: 37.66. Date:
Attendance number: 84. Patient Name: Demarcus Kris. Temperature: 37.12. Date:
Attendance number: 85. Patient Name: Phoebe Buckridge. Temperature: 38.64. Dat
Attendance number: 85 foward to the intensive care unit.
2020-06-10 05:10:50 26 entries.
Attendance number: 84. Patient Name: Demarcus Kris. Temperature: 37.07. Date:
Attendance number: 85. Patient Name: Phoebe Buckridge. Temperature: 38.67. Dat
Attendance number: 85 forward to the intensive care unit.
```

Figure 15. Patient record simulating discharge

If the patient's state remains feverish for five minutes, a message will be sent to the doctor in charge, as shown in Figure 16. If the temperature remains stable for ten minutes, the patient will be released.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2020 doi:10.20944/preprints202007.0369.v1

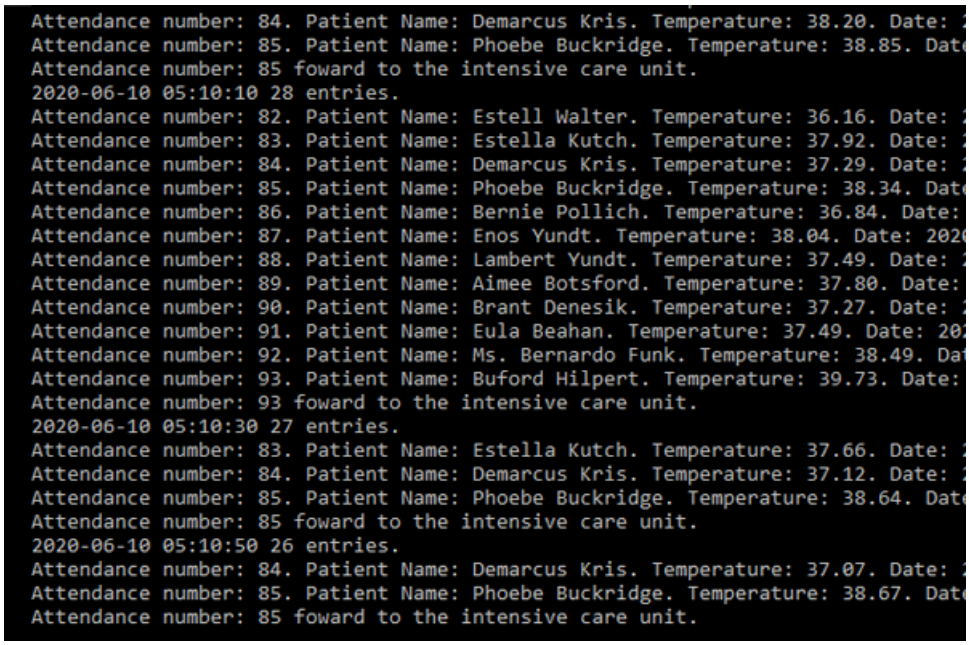

Figure 16. Registro do paciente simulando a entrada no atendimento médico

After testing and validating the application, it was possible to observe that the information flows through different devices. For the simulation environment, we tested with only one system that communicates with a wearable device. In real applications, there could be more than one device interacting with more than one system. However, the fluidity of the information would be similar: starting at the patient's registration at the time of admission to the emergency room; the system being accessed by the screening sector to insert health status data; receiving information from monitoring devices. At the time of the medical consultation, the system would receive more information regarding anamnesis, referrals for exams or hospital discharge. Given that the feverish state is strongly associated with a COVID-19 diagnosis, the patient should be constantly monitored and receive adequate care as long as the symptoms persist. The high contagion of the virus makes such care essential. The monitoring interval parameters, indicative of medical discharge or a possible carrier of the disease, are defined according to medical protocols. We emphasize that the interval and discharge suggestion present in this work are meant to simulate features.

7. Conclusions

After documenting the important steps at which data privacy is of the utmost importance in the emergency care process, particularly in a scenario that involves the COVID-19 virus, we developed a comprehensive taxonomy. It is branched into four items containing five attributes each; all of the items and their respective attributes are justifiable. For the information flow tests, we developed a prototype and application which, despite being simple, addresses the main questions about data privacy. The application was developed with registration data inputs and different choices of encryption/hash to be applied according to environmental criteria. The application communicates with a wearable that monitors the patient's temperature and provides treatment in line with the patient's feverish state, guiding the referral to the doctor's office or the possibility of discharge. With the application of taxonomic definitions as well as the agility of medical professionals in the care of patients with suspected COVID-19, the registration data is kept confidential through encryption and privacy requirements. Temperature monitoring should be done constantly; in the case of feverish states that persist for a period defined by the entity, along with other symptoms suggestive of the disease, the system suggests the referral of the patient without exposing personal data.

We believe that the research we have carried out contributes to several other studies currently in progress in several countries, which propose monitoring without consent and put forward definitions of use and data privacy criteria. For future work, we are developing improvements for privacy requirements that can be adapted to different countries, thus expanding the features of variable monitoring to identify patients with COVID-19 and obtaining new tests and results.

8. Acknoledgements

This work was partially supported by CAPES – Código de Financiamento (001). Este trabalho contou com apoio do projeto de cooperação internacional para desenvolvimento de pesquisas em gerenciamento de privacidade de dados Brasil / Portugal and by the project Smart following systems, Edge Computing and IoT Consortium, CONSORCIO TC_TCUE18-20_004, CONVOCATORIA CONSORCIOTC. PLAN TCUE 2018-2020. Project managed by Fundación General de la Universidad de Salamanca and co-financed with Junta Castilla y León and FEDER funds .

1. Doukas, C.; Maglogiannis, I. Bringing IoT and Cloud Computing towards Pervasive Healthcare. 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012, pp. 922–926. doi:10.1109/IMIS.2012.26.
2. Al-Odat, Z.; Srinivasan, S.; Al-Qtiemat, E.; Asha, M.; Dubasi, M.A.L.; Shuja, S. IoT-Based Secure Embedded Scheme for Insulin Pump Data Acquisition and Monitoring. 2018.
3. Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems* **2017**. doi:10.1016/j.future.2017.04.036.
4. Campos, J.; Souza, V.S.A. Percepção dos Usuários do Serviço de Urgência e Emergência em relação à classificação de risco pelo protocolo de Manchester. *Revista Unimontes Científica Montes Claros* **2014**, *16*. doi:http://www.ruc.unimontes.br/index.php/unicientifica/article/view/319/297, Acessado em 08/04/2020.
5. Rothan, H.; Siddappa, N. The epidemiology and pathogenesis of coronavirus disease (COVID-19) outbreak. *Journal of Autoimmunity* **2020**, *109*, 102433. doi:10.1016/j.jaut.2020.102433.
6. Soares, N.V.; Dall'Agnol, C.M. Privacidade dos pacientes: uma questão para a geração do cuidado em enfermagem. *Acta Paulista de Enfermagem* **2011**, *24*, 683 – 688. doi:10.1590/S0103-21002011000500014.
7. Barker, K.; Askari, M.; Banerjee, M.; Ghazinour, K.; Mackas, B.; Majedi, M.; Pun, S.; Williams, A. A Data Privacy Taxonomy. 2009, Vol. 5588, pp. 42–54. doi:10.1007/978-3-642-02843-4_7.
8. Asaddok, N.; Ghazali, M. Exploring the usability, security and privacy taxonomy for mobile health applications. 2017, pp. 1–6. doi:10.1109/ICRIIS.2017.8002472.
9. Coen-Porisini, A.; Colombo, P.; Sicari, S.; Trombetta, A. A conceptual model for privacy policies. 2007, pp. 570–577.
10. Silva, L.A.; Leithardt, V.R.Q.; Rolim, C.O.; González, G.V.; Geyer, C.F.R.; Silva, J.S. PRISER: Managing Notification in Multiples Devices with Data Privacy Support. *Sensors* **2019**, *19*. doi:10.3390/s19143098.
11. Leithardt, V.; Santos, D.; Silva, L.; Viel, F.; Zeferino, C.; Silva, J. A Solution for Dynamic Management of User Profiles in IoT Environments. *IEEE Latin America Transactions* **2020**, *18*, 1193–1199. doi:10.13140/RG.2.2.33091.63524.
12. Zwitter, A.; Gstrein, O.J. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action* **2020**, *5*. doi:10.1186/s41018-020-00072-6.
13. Yesmin, T.; Carter, M.W. Evaluation framework for automatic privacy auditing tools for hospital data breach detections: A case study. *International Journal of Medical Informatics* **2020**, *138*. doi:10.1016/j.ijmedinf.2020.104123.
14. Islam, S.M.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* **2015**, *3*, 678–708. doi:10.1109/ACCESS.2015.2437951.
15. Sun, J.; Zhu, X.; Zhang, C.; Fang, Y. HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare. 2011, pp. 373 – 382. doi:10.1109/ICDCS.2011.83.

16. Samaila, M.; Neto, M.; Fernandes, D.; Freire, M.; Inácio, P. Challenges of Securing Internet of Things Devices: A survey. *Security and Privacy* **2018**. doi:10.1002/spy2.20.
17. Hankerson, D.; Menezes, A.J.; Vanstone, S., Guide to elliptic curve cryptography; 2005; Vol. 46, p. 13.
18. Yi, X.; Bertino, E.; Rao, F.Y.; Bouguettaya, A. Practical privacy-preserving user profile matching in social networks. 2016, pp. 373–384. doi:10.1109/ICDE.2016.7498255.
19. Sivaraman, V.; Gharakheili, H.H.; Vishwanath, A.; Boreli, R.; Mehani, O. Network-level security and privacy control for smart-home IoT devices. 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2015, pp. 163–167. doi:10.1109/WiMOB.2015.73479565.
20. Fengou, M.; Mantas, G.; Lymperopoulos, D.; Komninos, N. Ubiquitous Health Profile Management Applying Smart Card Technology. 2011, Vol. 83. doi:10.1007/978-3-642-29734-2_34.
21. Leithardt, V.; Borges, G.; Rossetto, A.; Rolim, C.; Geyer, C.; Correia, L.; Nunes, D.; Sá Silva, J. A Privacy Taxonomy for the Management of Ubiquitous Environments. **2013**.
22. V., D.V.; Senthilkumar, S. HB-PPAC: hierarchy-based privacy preserving access control technique in public cloud. *International Journal of High Performance Computing and Networking* **2017**, *10*, 13. doi:10.1504/IJHPCN.2017.10003759.
23. Ibraimi, L.; Asim, M.; Petković, M. Secure Management of Personal Health Records by Applying Attribute-Based Encryption. 2009, pp. 71 – 74. doi:10.1109/PHEALTH.2009.5754828.
24. Centers for Medicare & Medicaid Services. The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Online at http://www.cms.hhs.gov/hipaa/, 1996.
25. Costa, R.G.R. Apontamentos para a arquitetura hospitalar no Brasil: entre o tradicional e o moderno **2011**. *18*, 53 – 66. doi:10.1590/S0104-59702011000500004.
26. Lopes, S. Privacidade dos dados em ambientes de interoperabilidade – a área da saúde. PhD thesis, Universidade de Évora, 2016.
27. Poleto, T.; Silva, L.C.; Carvalho, V.D.H.; Moura, J.A.; Costa, A.P.C.S., Modelo de Decisão para Identificação e Priorização de Politicas de Segurança de Informação em um Hospital Público; 2015.
28. Yeniman Yildirim, E.; Akalp, G.; Aytac, S.; Bayram, N. Factors Influencing Information Security Management in Small- and Medium-Sized Enterprises: A Case Study from Turkey. *Int. J. Inf. Manag.* **2011**, *31*, 360–365. doi:10.1016/j.ijinfomgt.2010.10.006.
29. Florence, G.; Saide, J.; Calil. Uma nova perspectiva no controle dos riscos da utilização de tecnologia médico-hospitalar **2005**.
30. Machado, D.; Doneda, D., Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados; 2019; pp. 99–125.
31. Lei Geral de Proteção de Dados Pessoais (LGPD), 2018. [acessado em 21/03/2020].
32. Lupiana, D.; O'Driscoll, C.; Mtenzi, F. Taxonomy for ubiquitous computing environments. *2009 First International Conference on Networked Digital Technologies* **2009**, pp. 469–475. doi:10.1109/NDT.2009.5272068.
33. Pradilla, J.; Esteve, M.; Palau, C. SOSFul: Sensor Observation Service (SOS) for Internet of Things (IoT). *IEEE Latin America Transactions* **2018**, *16*, 1276–1283. doi:10.1109/TLA.2018.8362168.
34. Fowler, M. *UML Essencial: Um Breve Guia para Linguagem Padrao*; Bookman, 2005.
35. Menezes, A.J.; Vanstone, S.A.; Oorschot, P.C.V. *Handbook of Applied Cryptography*, 1st ed.; CRC Press, Inc.: USA, 1996.
36. Singhal, T. A Review of Coronavirus Disease-2019 (COVID-19). *The Indian Journal of Pediatrics* **2020**, *87*. doi:10.1007/s12098-020-03263-6.